Western Digital.

De-risking Data with Smarter Storage

New research explores today's data risks, storage challenges and IT leaders' plans to mitigate them

Data is valuable – which means when storing and sharing it, risk must be taken into account.

But that risk is being increasingly exacerbated by a number of factors, including a changing threat landscape, a lack of appropriate data security tools, and insecure internal storage and sharing practices.

Combined, these challenges have created a security pinch point for data security decision makers (hereafter data manager). Across the board, this group believe that **data security could be improved – particularly in how their organisations store and transmit sensitive data.**

Fortunately, there are strategies and solutions data managers can employ to overcome their challenges. With smarter storage technologies, data managers can protect their work and their businesses. With the right tools, they can improve how sensitive data is stored, communicated and moved – and by educating employees on safe data habits, they can create a culture of true data security.

But what do those technologies, strategies and habits l ook like? To understand more about current data managers challenges and how the situation could be improved, Western Digital commissioned an in-depth research project to get a 360 view of the attitudes and behaviors around sensitive data storage.

The Facts Behind the Figures

This research was conducted among 737 data managers and 1,467 data users across the UK, Italy, France, Germany, Spain, Saudi Arabia and the UAE during summer 2021. Data managers were defined as data security decision makers, while data users were defined as employees that work with or create highly sensitive data. Highly sensitive data includes but is not limited to research and development data, production data, or client, citizen, and patient data (e.g. medical records, financial and personal data.)

Respondents worked in media and entertainment, the public sector, legal professional services, healthcare and financial services, and in businesses ranging in size from small (10–99 employees) to enterprise (5000+ employees).

The Data Storage Challenge

To establish what businesses really need from their secure data storage solutions, it's important to understand what challenges data managers are facing – and where the threats are coming from.

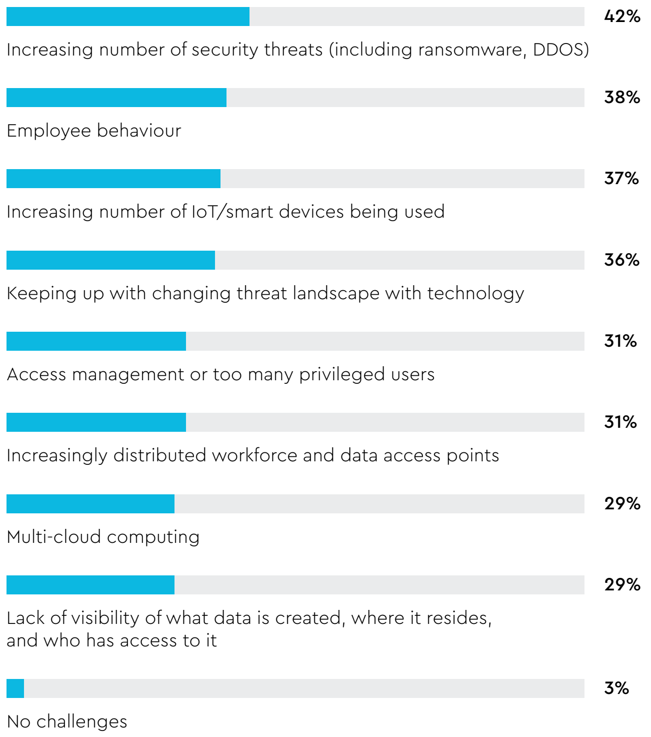
As Fig.1 shows, the increasing amount of security threats is concern felt by the largest number of data managers. But while this is undoubtedly worrying, the growing variance of external threats can't always be controlled from within the business.

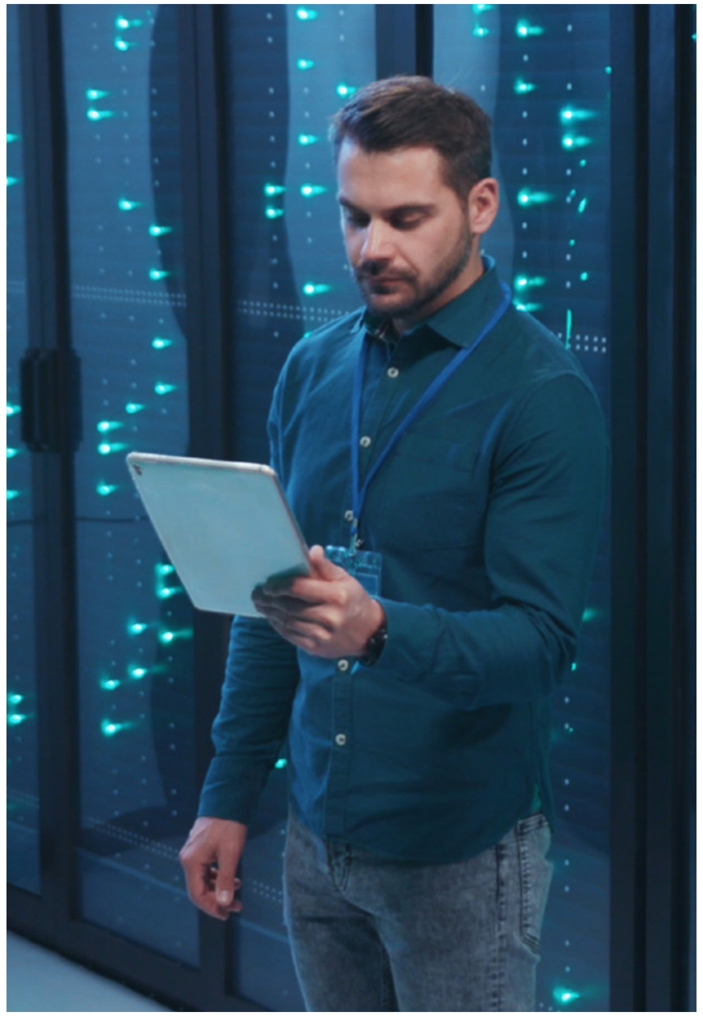
What data managers can address are issues around employee behavior, devices, and the tech landscape. From the growing number of devices used within a business to an increasingly distributed workforce, data managers face spiraling complexity (62% of the data manager respondents state that threats and incidents have increased over the past 12 months). It's also worth noting that, while growing security threats are the number one concern in general, two thirds of data managers (68%) say employee behavior is an overall bigger threat to their highly sensitive data than external hackers.

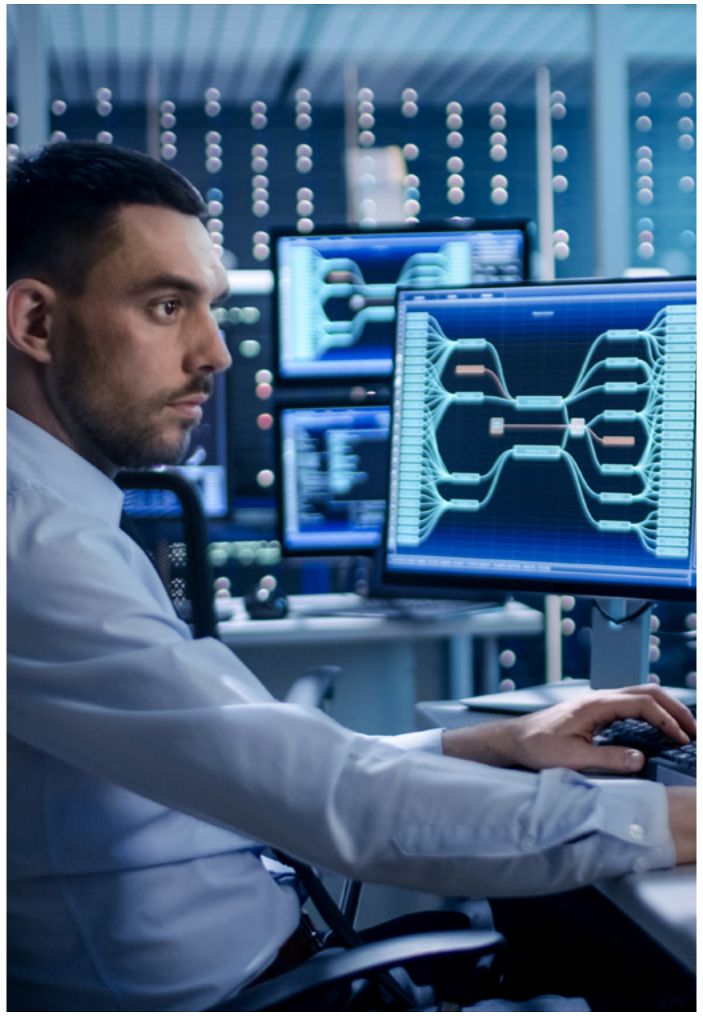
In short: it's internal data management, rather than external threats, that data managers should move to address most urgently – not least because they can make a bigger impact.

Fig.1

Which of the following do you see as the key data security challenges in your organization currently?







How data is stored and shared today

As the internal or behavioral threat of data storage and sharing becomes more prevalent, there is an opportunity for businesses to use every tool at their disposal to boost security – whether that's the most secure technology, encryption, or investing in education.

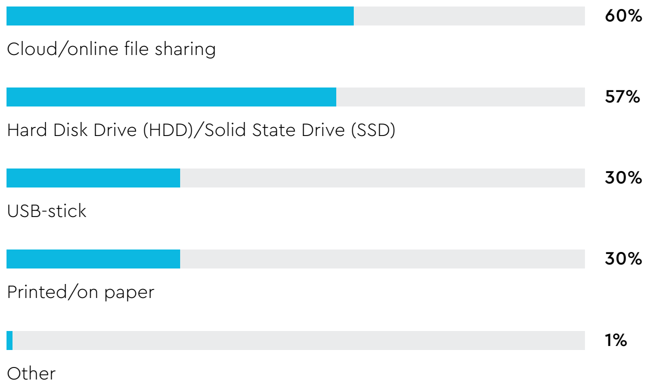
But at present, there is a clear disconnect between what data managers think they should be doing and what they are doing.

For example, while data managers identify Hard Disk Drive (HDD) or Solid State Drive (SSD) as the most secure and recommended approach to storing sensitive data, it's not currently the most-used tactic. (Fig.2).

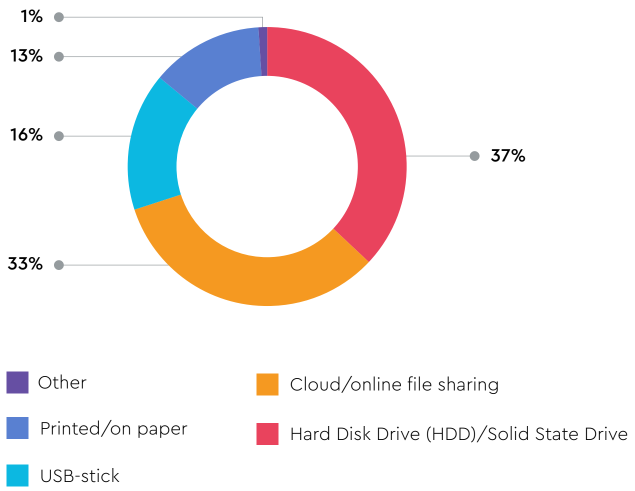
Fig.2

In which of the following ways is highly sensitive data stored in your organization? / Which of these do you see as the most secure and would you recommend to employees for storing highly sensitive data?

Methods for storing highly sensitive data in organization



Method seen as most secure and recommended to employees for storing highly sensitive data

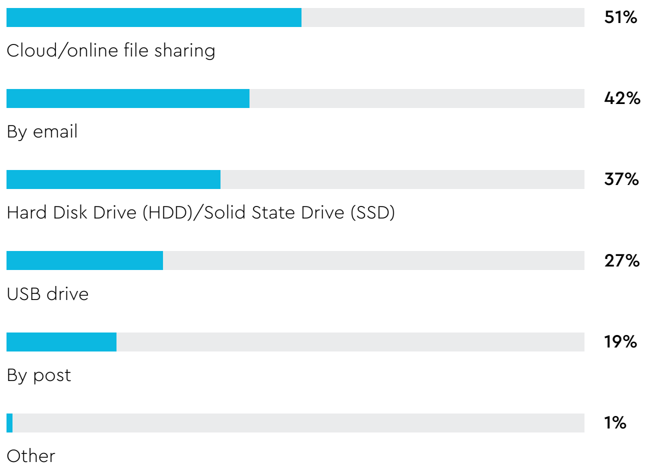


Likewise, only 37% of data users utilize HDDs and SSDs for sharing data. There are some worrying conflicts elsewhere; email is the second most popular method of sharing, despite only 13% of data managers thinking this is the most secure/recommended way to work.

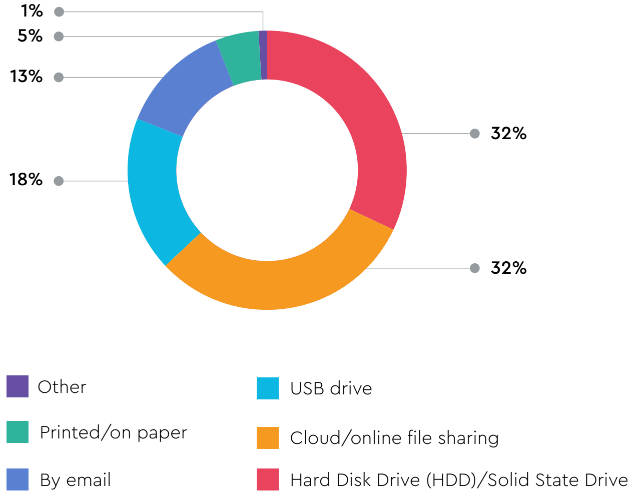
Fig.3

In which of the following ways is highly sensitive data stored transmitted / shared by your organization? / Which of these do you see as the most secure and would you recommend to employees for sharing/transmitting highly sensitive data?

Method for sharing highly sensitive data in organization



Method seen as most secure and recommended to employees for sharing highly sensitive data



If data managers are going to address security and storage challenges in the long-term, businesses and data users need to start aligning their strategies to what they know to be effective – especially as the employee risk grows.

Understanding Employee-based Risk

On average, 28% of today's data security incidents originate with employees – rising to 36% in the UAE and 31% in the UK. In addition, 26% of employees are estimated to have put sensitive company data at risk over the past 12 months.

That means that over a quarter of the workforce has potentially compromised the security and prosperity of the organizations they work for. The pandemic and home working has heightened this trend: 35% of data managers think employees lack the tools/technology to safeguard data at home, and 33% think employees feel psychologically more 'removed' from risks while working remotely. Meanwhile, 32% think there's simply a lack of clear guidance for employees. All of which adds up to a growing problem for data security and storage.

Understanding the internal risk

As Fig.4 shows, data managers believe there are myriad contributors to the rising internal threat to data security. Ranging from the old (but everlasting) problem of poor password hygiene, to the alarming issue of employees not fully knowing what constitutes sensitive data, or the consequences to their business if they lose it.

Fig.5 expands on this trend, showing that although employee understanding is relatively good around data sensitivity, it's rarely excellent. 71% of employees say they have never knowingly put company data at risk, but some simply don't know what constitutes sensitive data, or what to do with it.

Fig.4

To what extent do you think the following present internal data security risks in your organization currently?

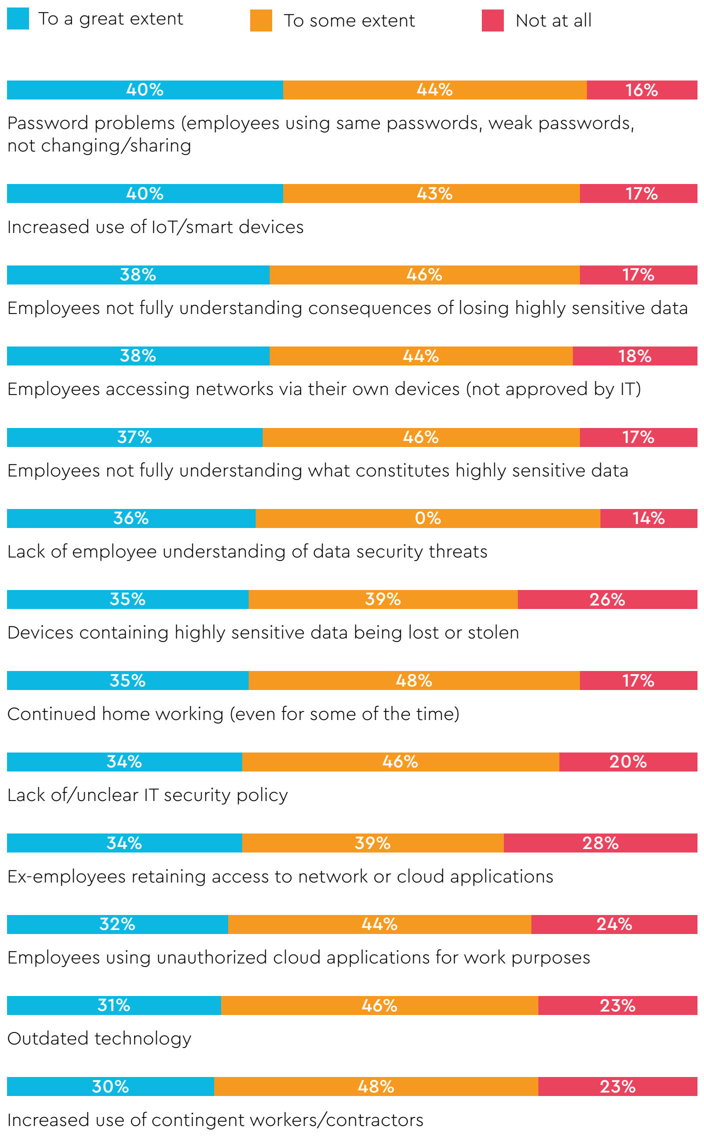
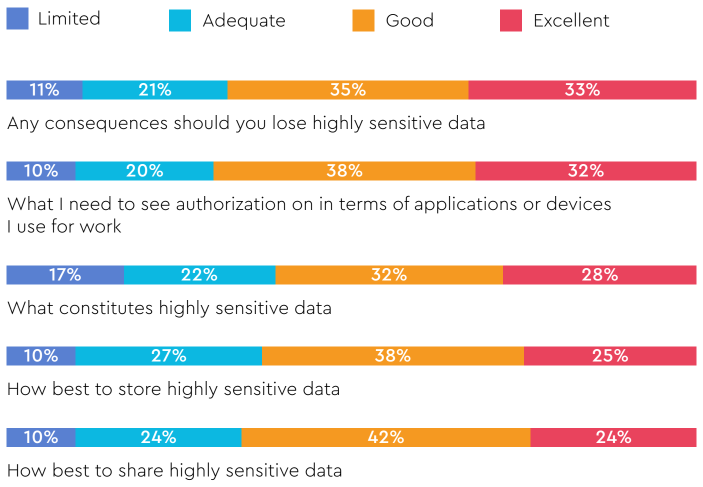


Fig.5

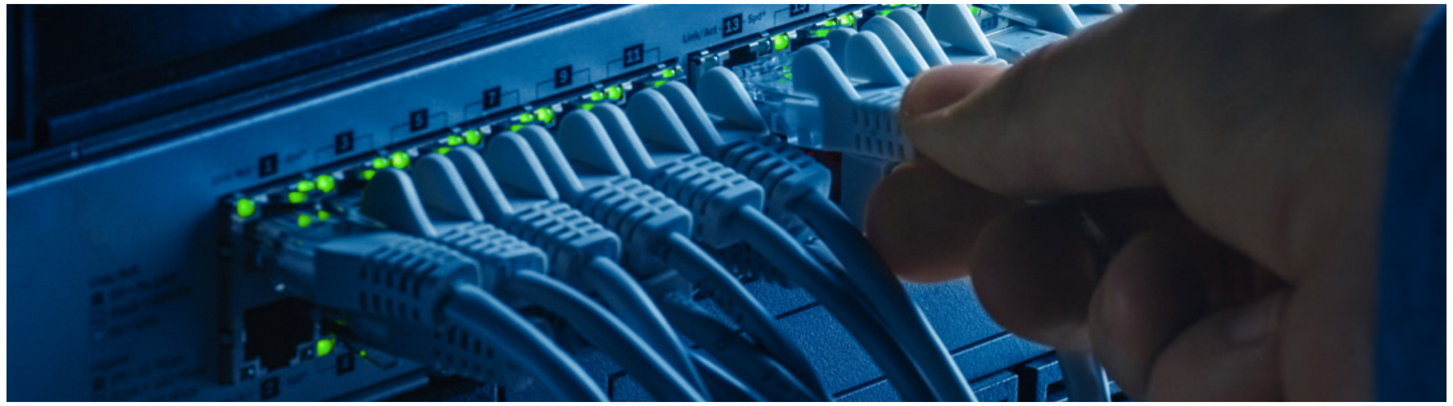
Please rate your understanding of the following at work.



The question is, what can data managers do about this?

Some will look at issues posed by the cloud (as we'll go on to explore), but avoiding the cloud isn't really an option – particularly with the continued rise of hybrid working.

Instead, data managers must look for smarter, more resilient and employee friendly solutions that remove the reliance on passwords altogether, while also encouraging better habits and behaviors with sensitive data.



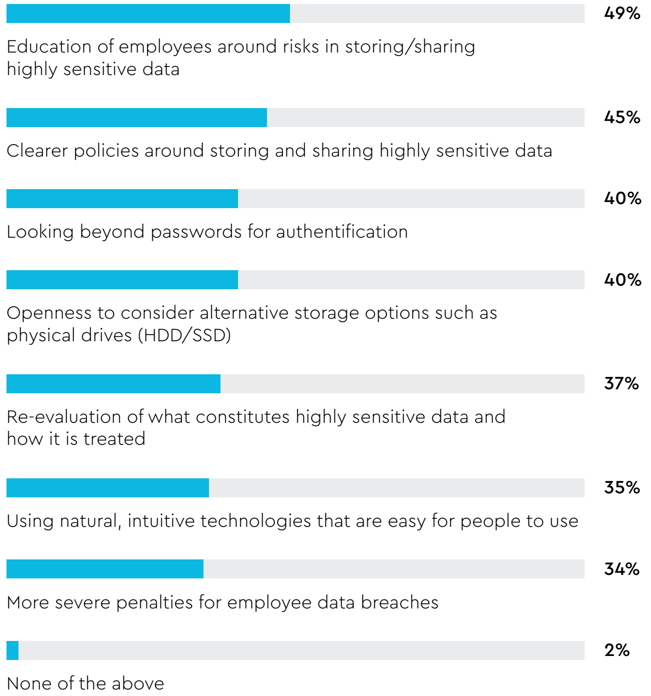
Smarter Storage, Stronger Security

The research also shows widespread agreement among data managers that highly sensitive data security needs improvement when it comes to storage and transmission (61% say it definitely needs improvement, 37% probably).

Fig.6 unpacks this, showing that education about the risks of storage and sharing, clearer policies, going beyond the password, and alternative physical solutions like HDDs and SSDs are the preferred ways of improving security.

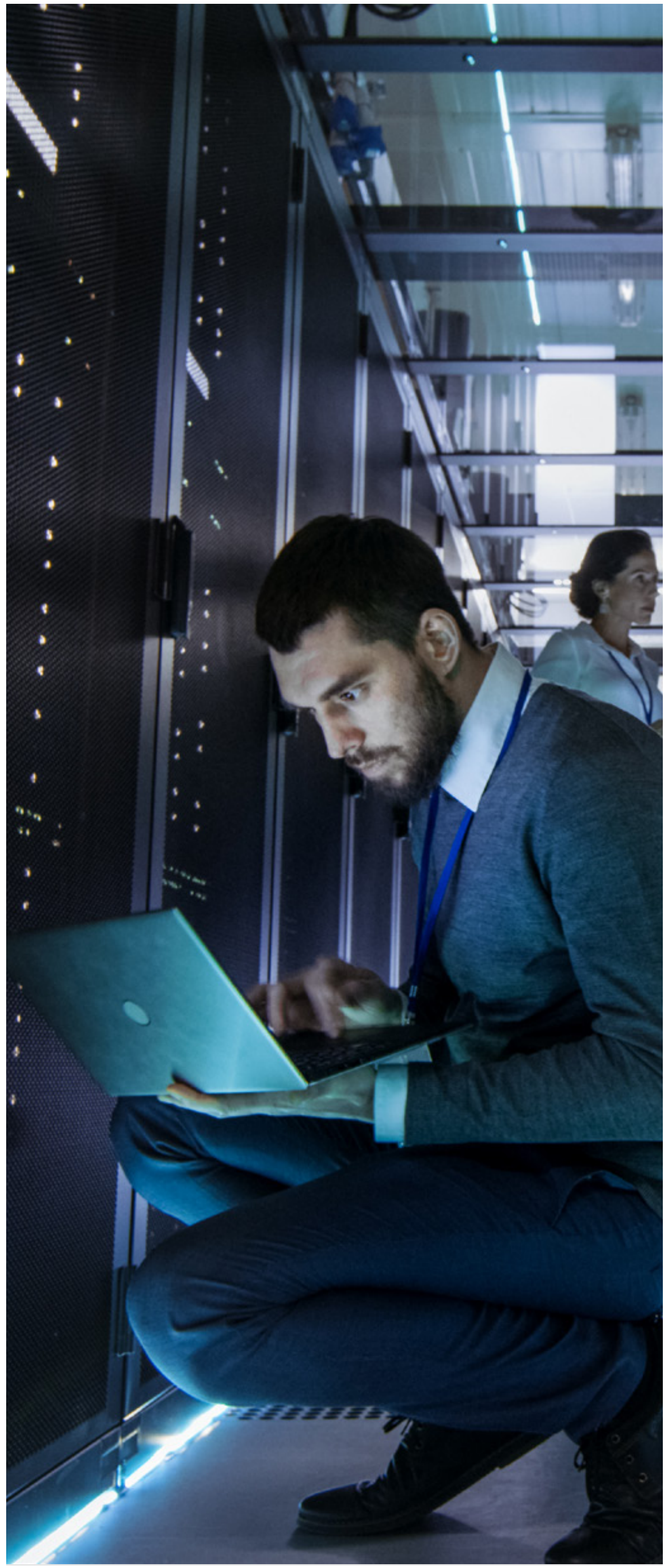
Fig.6

In what ways do you think the storage and transmission of highly sensitive data could be improved in your organization?



This highlights that data managers see two primary ways to address the myriad data security threats that dominate their time:

1. Improve employee behavior to stop risk-fraught practices
2. Acquire advanced solutions that mitigate risk, even if employee behavior doesn't improve



The future for physical solutions

While cloud storage has a role to play for most (if not all) businesses today, there's no getting around the fact that data managers aren't always comfortable with it:

- 87% say that data breaches and leaks are a significant or moderate concern about cloud
- 84% are worried about insecure transmission paths
- 80% are concerned about insufficient speed for large data volumes

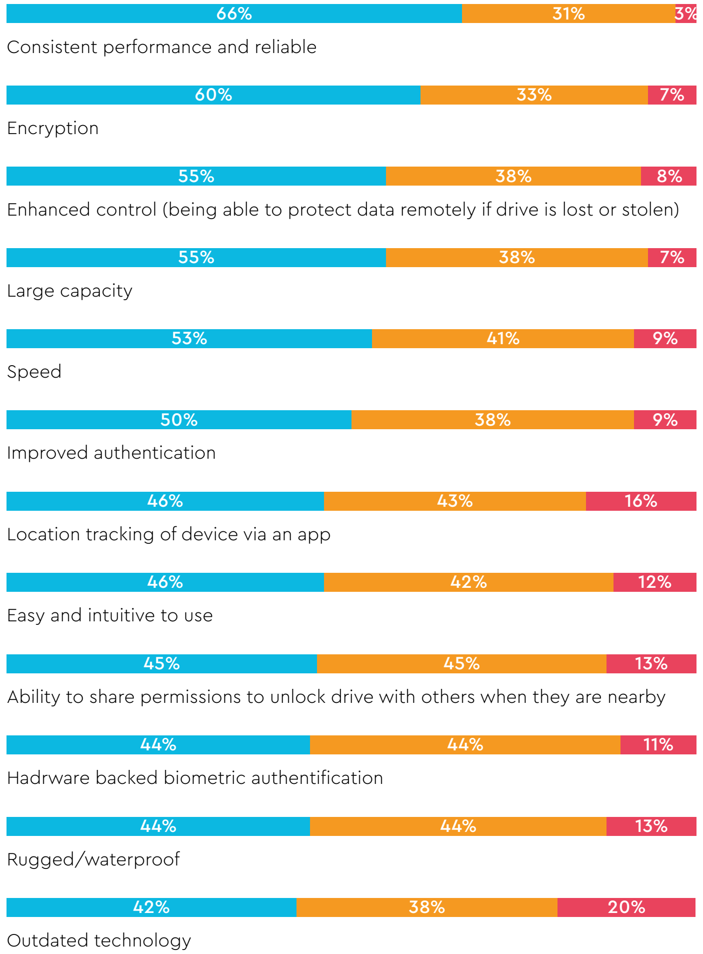
In short: cloud can be an excellent solution in many cases. For others, businesses may need alternatives.

This, and the belief that data security needs immediate improvement, is partly why the majority (54%) of data managers intend to increase their use of HDDs and SSDs over the next two years. And while some may have had concerns about this approach historically, three quarters (76%) say that 'HDDs or SSDs with encryption or security features address many of the concerns we have about this kind of technology.'

In the simplest terms, as their risk vectors evolve and data security and storage becomes more complex, data managers know they have to react. Most are now looking for the best partners with the best tools to do the job (Fig.7 shows the feature list they're looking for), helping them keep hackers at bay, improve internal behaviors and standards, and give highly sensitive data the high performing security it requires.

Fig.4

To what extent do you think the following present internal data security risks in your organization currently?



The Employee View

Data users represent a far greater risk than ever before. In part, that's down to hackers getting smarter and more sophisticated in how they target employees. It's also a result of an overnight switch to remote working, which rapidly increased the use of personal devices for work tasks, and separated employees physically from their IT teams.

However, there's no getting around the fact that poor password habits and a lack of knowledge are also issues. Fortunately, employees demonstrate both the will and desire to improve how they work with sensitive data. The employee view is outlined in the following findings:

The Downside

- 61% of data users say that encryption is necessary and has no impact on their experience, but 34% say it makes access and transmission harder (5% don't even know what it is)
- 83% only change passwords when they have to, 64% use the same or similar passwords for multiple things, and 62% write theirs down
- 69% give HDDs and SSDs to other people at work to share data

The Upside

- 67% say HDDs and SSDs feel more secure than cloud for storing highly sensitive data
- 78% recognize that the impact of a breach is more severe than ever
- 77% want to know more about data security and the different threats that exist

Your Next Storage Solution

Security around highly sensitive data is a perennial challenge – but as this research demonstrates, it's also an evolving one, particularly in terms of employee behaviors and the internal risk.

No IT leader wants to see their business mentioned in a headline about a data breach. Particularly when it could've been avoided through a combination of education, policy and technology. So, it's now down to IT leaders to protect their businesses, empower their data managers and help their employees. Manage this, and businesses can ensure that data stays where it should – and today's risk doesn't turn into tomorrow's breach.

Five key findings from this report:

Employee behavior is a significant data challenge:
68% of data managers believe it is a bigger threat to highly sensitive data than external hackers, while one in four data security incidents are estimated to have originated with employees

Remote and hybrid working styles have exacerbated data storage and security challenges:
35% of data managers think employees lack the tools/technology to safeguard data at home, while 33% feel psychologically more 'removed' from risks while working remotely

A 'should do' / '**actually** do' disconnect exists:
data managers identify HDDs and SSDs as the most secure, recommended way to store data – but this isn't the most widely used approach

Cloud is a concern:
although cloud is commonly used to share and store data, nine in ten (87%) say that data breaches and leaks are a significant or moderate concern

Despite the challenges, data managers do see a solution:
54% plan to increase their use of HDDs or SDDs in the next two years, and 76% think HDDs or SSDs with encryption or security features would address many of the concerns they have about the technology

Western Digital.

The ArmorLock™ technology solution from Western Digital is a revolutionary new security platform that's specifically designed to help data managers with today's storage challenges. Find out more about how the G-DRIVE™ ArmorLock SSD with next-generation security and simplicity can help you find a smarter, more secure way to store sensitive data.

WWW.WESTERNDIGITAL.COM/CONTACT