The Era of Hybrid Cloud Storage

How AI and cybersecurity considerations
are shaping enterprise storage strategies

2025 Edition

≡NASUNI

Contents

76% are planning to implement a hybrid cloud storage model within 12 months

#1 concern when managing file data infrastructure is security

53% say their data isn't backed up, immutable, and easily recoverable

92% have found extra budget for AI initiatives

5 weeks is the average time taken to recover from a cyberattack

Introduction

Worldwide, enterprises have embraced hybrid cloud. In fact, as many as three-quarters of organizations deploy a combination of private and public cloud[1].

The flexibility and resilience of a hybrid model helps to increase IT efficiency, ensure business resilience, and reduce costs while enabling scalability and better data management. It's also a vital factor in accessing and sharing data to fuel the widespread adoption of AI, including large language models (LLMs), agentic AI, and machine learning.

While some elements of firms' cloud strategy are integrated, an area that still shows signs of disconnect is data storage. The explosion in unstructured data requires companies to move away from a hardware-centric model in order to get the most out of their data.

1 www.statista.com/statistics/1472474/hybrid-cloud-strategies-global/

We surveyed a thousand purchasing decision makers in the US, UK, France, and DACH regions to understand attitudes towards data storage, security, and AI in the hybrid cloud era.

A number of key themes emerge from survey results:

- Firms are shifting data to the cloud to improve business resilience and data security. **Almost three-quarters of firms either have or are planning to implement a hybrid cloud storage model within 12 months.**

- Organizing and unifying data will be imperative for those planning AI initiatives: **currently only one-fifth are confident their data is AI-ready.** And on the whole, the larger the company, the worse the problem becomes.

- **AI tops the list of both current and future investment priorities.** In addition to raising extra budget, around one-fifth of firms are shifting money away from other areas to fund AI initiatives.

- Misplaced confidence is threatening firms' cybersecurity. **Nearly two-thirds say they're confident they can recover critical unstructured data and cope with a destructive cyberattack – but the data shows that in reality 45% struggled to do so.**

Organizations are adopting hybrid cloud strategies to better protect their data, collaborate more efficiently, and deliver on their AI and innovation plans. Our hope is that the findings in this report will help you ensure your own data management strategy is fit for purpose in 2025 and beyond.

Methodology
This survey was conducted among 1,000 purchasing decision makers, across the US, UK, France, and DACH regions (Germany, Austria, Switzerland), in organizations with 1,000+ employees. The interviews were conducted online by Sapio Research in January 2025 using an email invitation and an online survey.

What do we mean by hybrid cloud storage?

Hybrid cloud storage blends the scalability advantages of cloud-based object storage with local performance delivered via intelligent file caching at the edge and integrated data security, all in a single, unified platform.

This combination provides unlimited scale to support business growth while providing a file data platform that supports solutions like AI services.

Section 1:
The cloud context

The pace of cloud adoption and what's triggering organizations to invest.

Financial services sector leads cloud adoption

Organizations recognize the benefits of the cloud, but adoption rates are impacted by industry-specific considerations.

Financial services firms, whose customers expect agile digital services, top the chart – with 96% of those we surveyed already supporting cloud infrastructure.

By contrast, energy, oil, and gas companies, whose dispersed facilities and legacy networks can slow digital transformation, sit near the bottom, alongside retail and consumer goods firms.
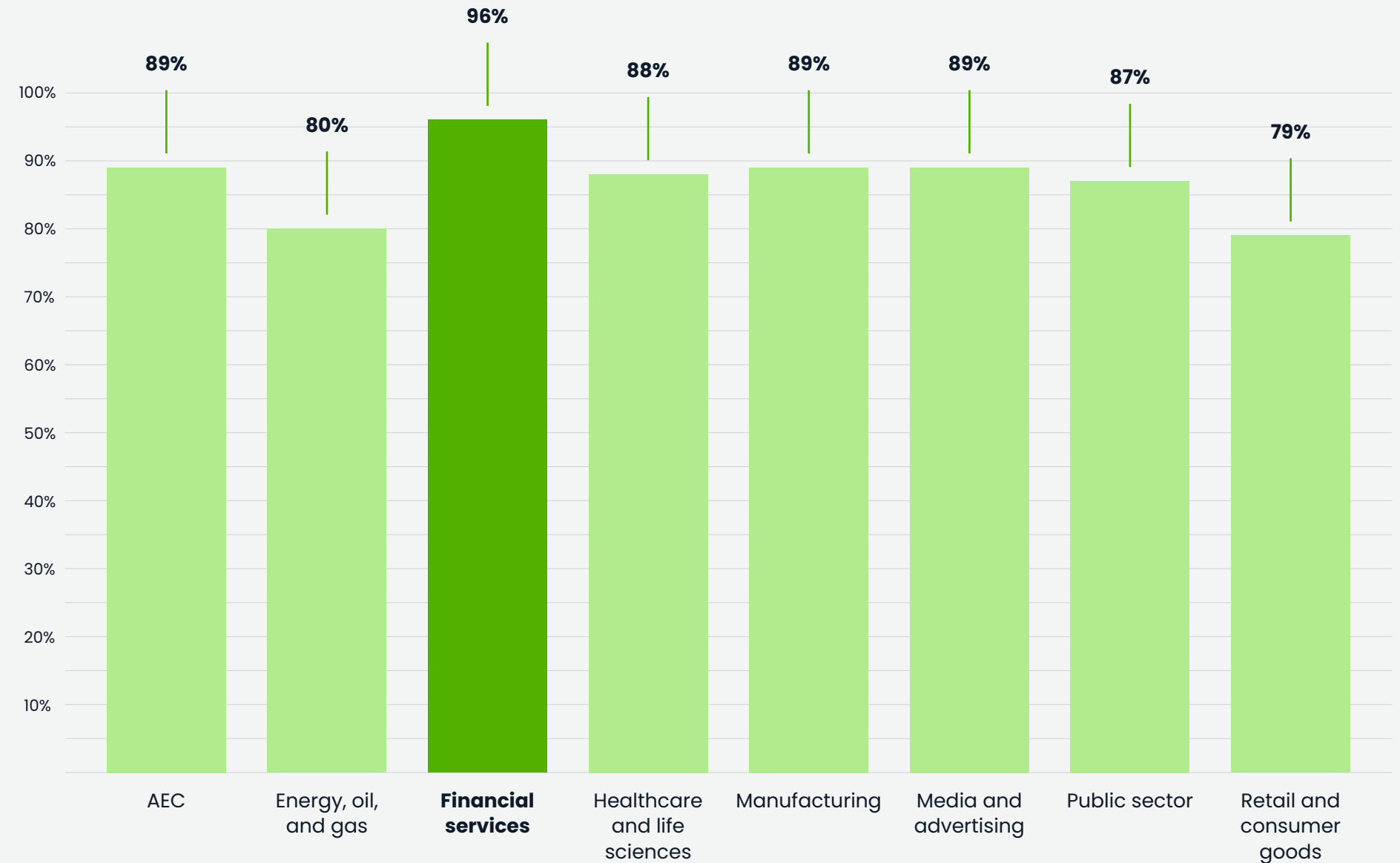
1,000 respondents were asked if their company currently supports a cloud or hybrid cloud infrastructure.

Around half of organizations prioritize AI investment

Nearly half (47%) of respondents cite AI as their top spending priority today, and more than a third (38%) say it will stay that way for the next 18 months.

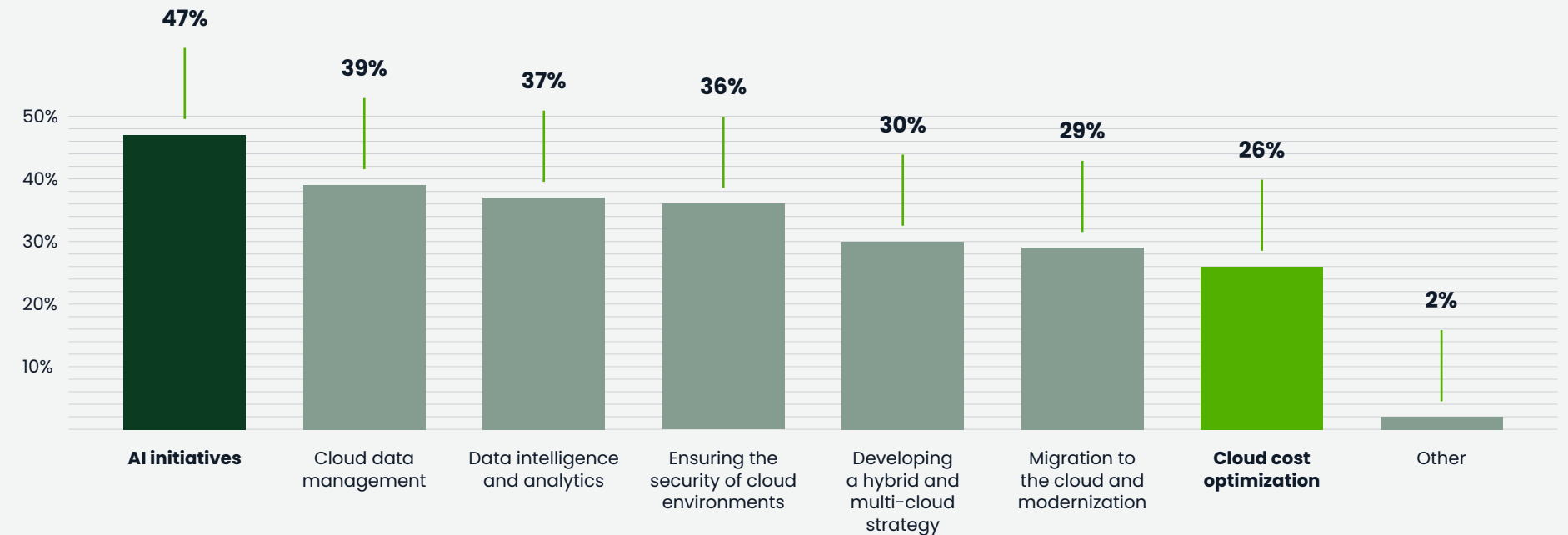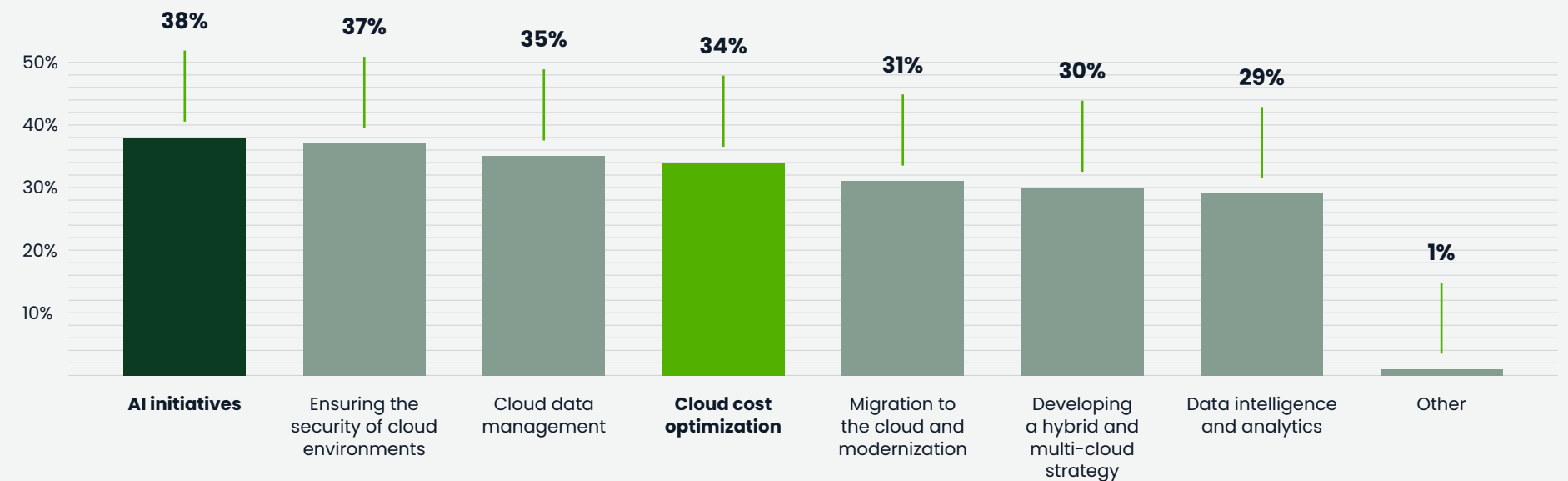In order to support innovation, however, firms will need to make savings elsewhere. Cloud cost optimization is set to shift up the priority list by three places over the next year and a half.

Continued pressure on budgets due to rising prices and the changing geopolitical landscape means firms anticipate a growing need to optimize spending.

1,000 respondents were asked to select their businesses' current investment priorities.

	%
AI initiatives	47%
Cloud data management	39%
Data intelligence and analytics	37%
Ensuring the security of cloud environments	36%
Developing a hybrid and multi-cloud strategy	30%
Migration to the cloud and modernization	29%
Cloud cost optimization	26%
Other	2%

1,000 respondents were asked to select their businesses' planned investments in the next 18 months.

	%
AI initiatives	38%
Ensuring the security of cloud environments	37%
Cloud data management	35%
Cloud cost optimization	34%
Migration to the cloud and modernization	31%
Developing a hybrid and multi-cloud strategy	30%
Data intelligence and analytics	29%
Other	1%

> Businesses are increasingly exploring the use of hybrid cloud and multi-cloud strategies to improve their cybersecurity risk posture.

TechTarget, The future of hybrid cloud:
What to expect in 2025 and beyond

Cloud infrastructure is key to business resilience

The #1 benefit of a cloud infrastructure strategy is better data security and business resilience, closely followed by the efficiencies that derive from more streamlined processes.

45%
44%
35%
33%
25%

Improving data security and business resilience

Streamlining processes to improve business efficiency

Building a compelling AI strategy

Improving customer experience

Meeting sustainability goals
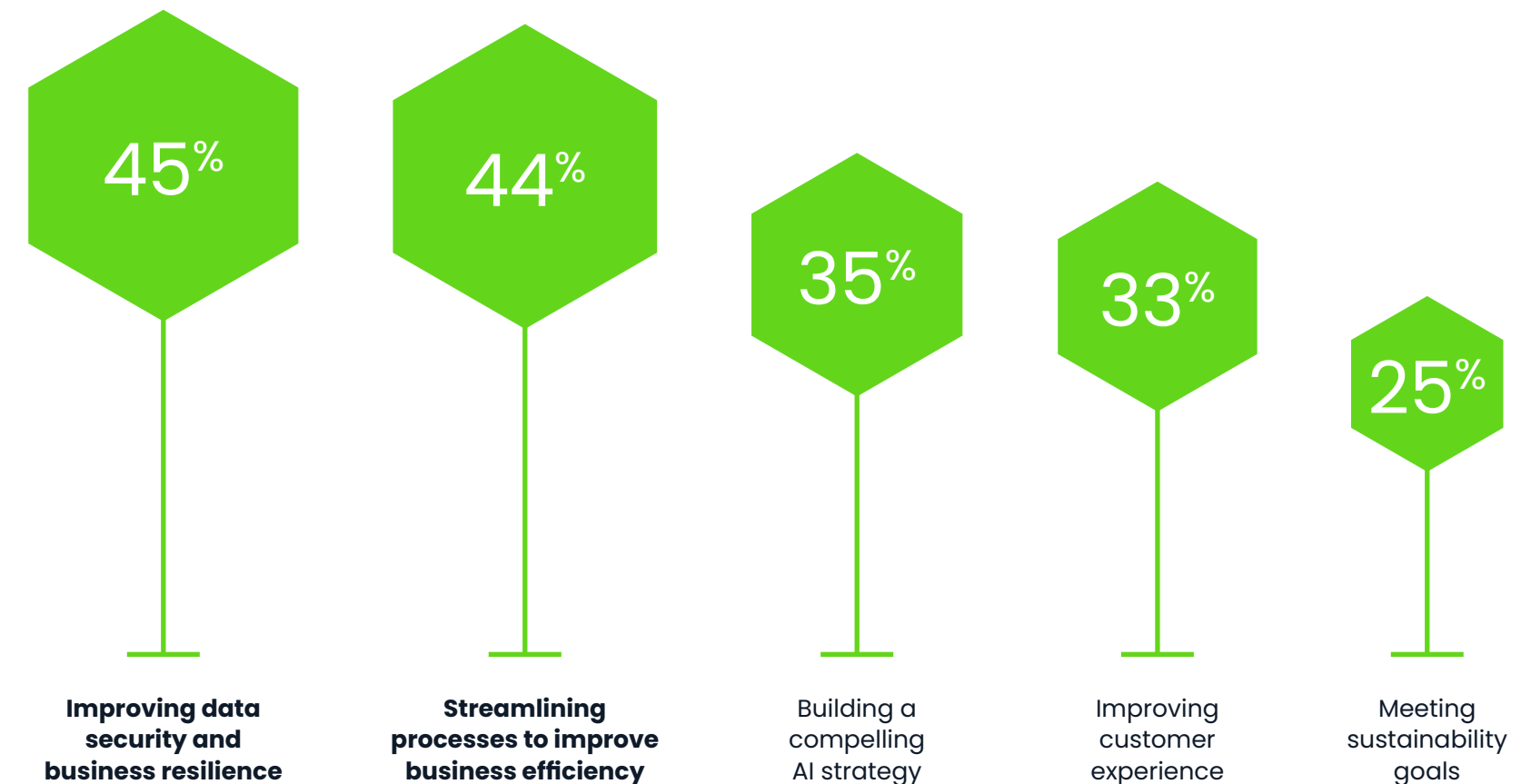
1,000 respondents were asked which business goals their cloud infrastructure strategy is supporting / going to support.

Section 2:
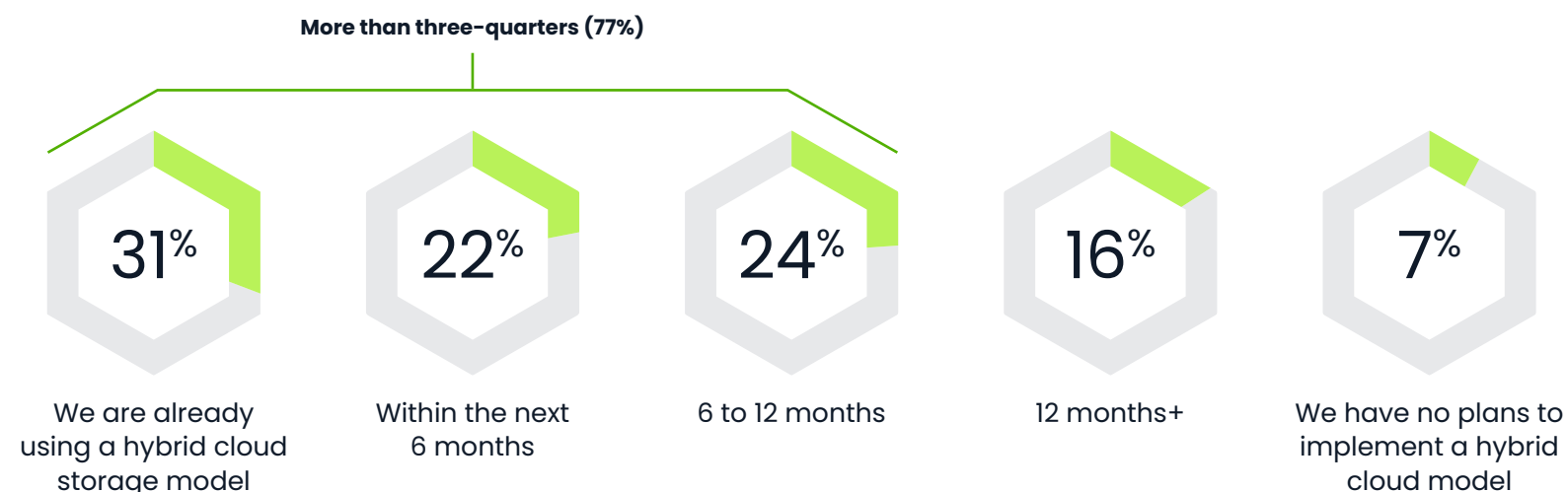# Trends in data storage

The strategies organizations are adopting to deal with increasing volumes of data and data silos.

Three-quarters will have hybrid cloud storage within the year

As companies' cloud strategies become more sophisticated, data storage must follow suit.

More than three-quarters (77%) are either using a hybrid cloud storage model or planning to within the next twelve months. Fewer than 10% have no plans to introduce a hybrid model.

Given that financial services are most likely to have shifted to cloud or hybrid cloud, it makes sense that this sector is most likely (44%) to have a hybrid storage model, while public sector (23%) and energy, oil, and gas (22%) are least likely.

More than three-quarters (77%)

31%	22%	24%	16%	7%
We are already using a hybrid cloud storage model	Within the next 6 months	6 to 12 months	12 months+	We have no plans to implement a hybrid cloud model

1,000 respondents were asked when, if at all, their business plans to implement a hybrid cloud storage model.

" The data storage market faces evolving challenges in enterprise IT. With emerging trends of exponential data growth, public cloud integration, talent acquisition hurdles, emerging workloads, cyberthreats, and the rise of generative AI, modern adaptable storage platforms will be in high demand.

Consumption models are changing the way clients source and manage storage infrastructure. Generative AI presents unique challenges as it has a potential to generate large amounts of data, requiring highly performant, scalable, and sustainable storage solutions. Security and privacy concerns associated with generative AI content also require robust cyberstorage platforms.[2]

Gartner®, Hype Cycle for Storage Technologies, 2024

2 Gartner®, Hype Cycle for Storage Technologies, 2024, Analyst Julia Palmer, 10 July 2024
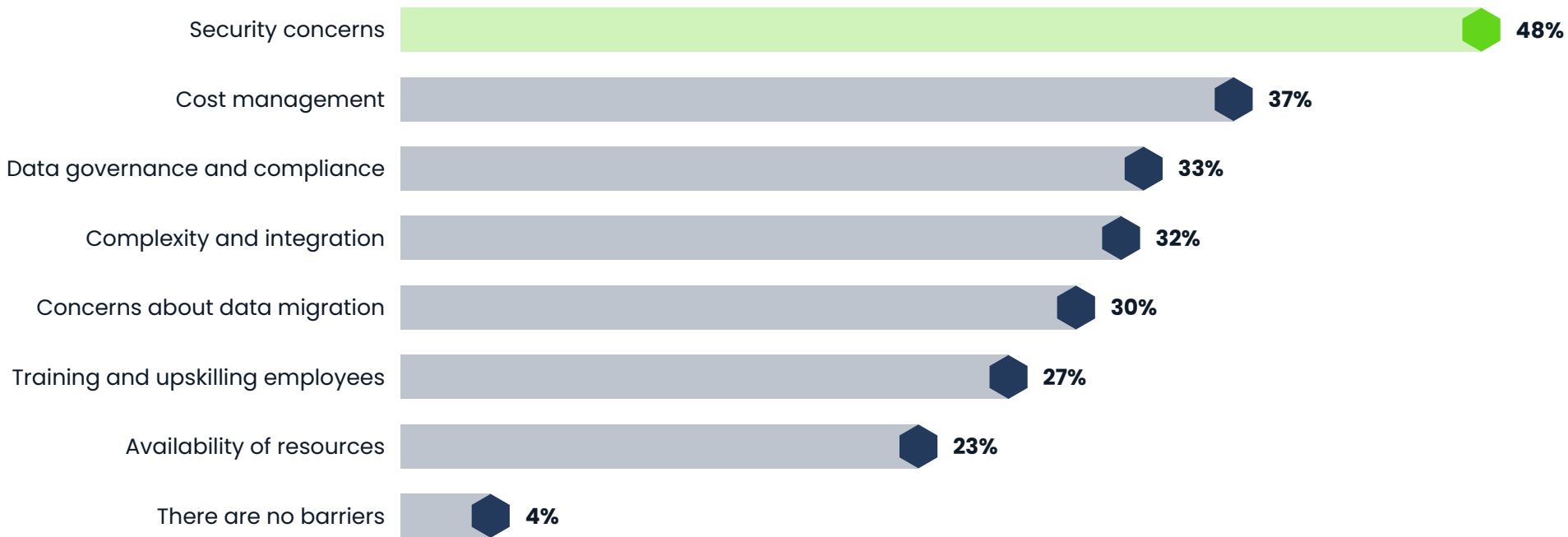
Security tops list of file data challenges and concerns

Against a backdrop of technological change, one thing remains constant — the struggle to keep data secure.

In 2024, our report[3] found that security concerns were the top reason firms hadn't moved data into the cloud — and also the top challenge when managing file data. This year's findings tell a similar story.
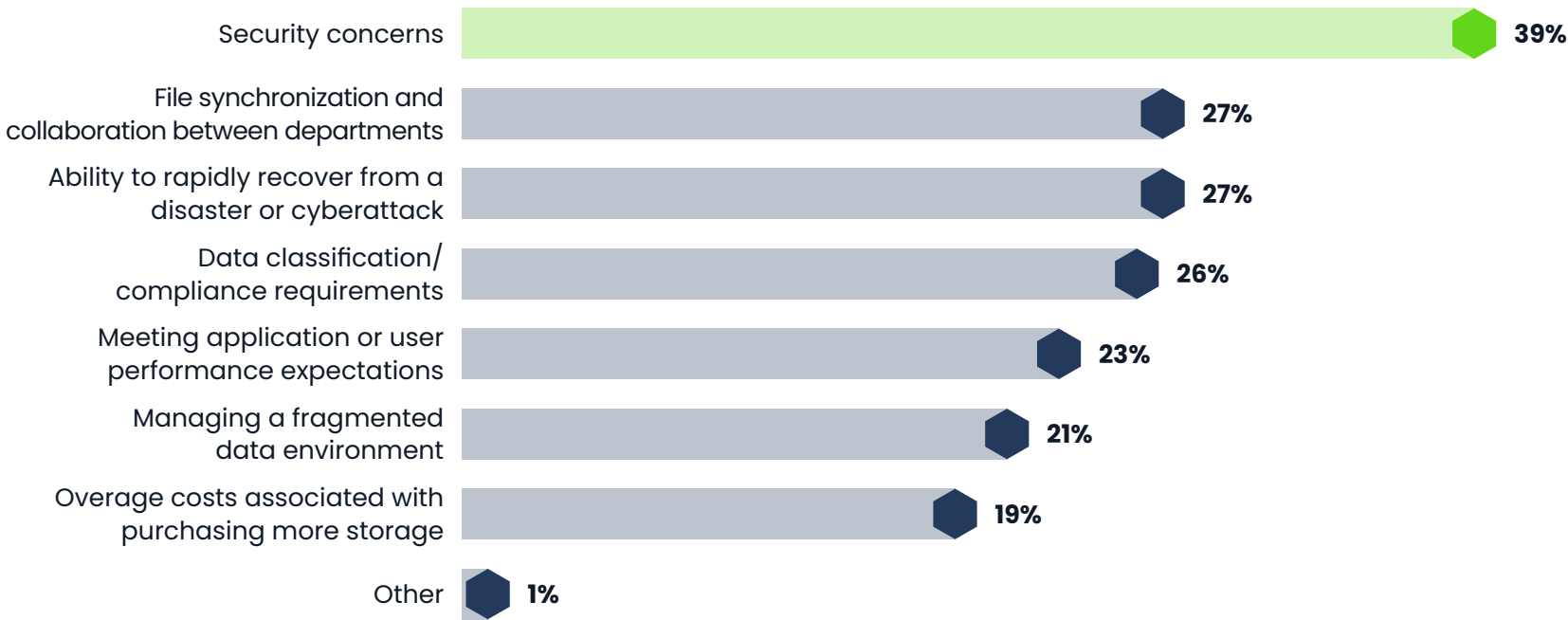
Just under half of respondents (48%) see security as a main blocker to moving file data to the cloud.

Organizations are struggling to balance making data available to the right people at the right time, while keeping it safe. **The top concern when managing file data infrastructure is security,** followed by facilitating interdepartmental collaboration, and speed of recovery from cyberattacks.

---

3 Please note the 2024 report surveyed a different demographic selection, which means direct comparisons can't be drawn.

Challenge	%
Security concerns	48%
Cost management	37%
Data governance and compliance	33%
Complexity and integration	32%
Concerns about data migration	30%
Training and upskilling employees	27%
Availability of resources	23%
There are no barriers	4%

1,000 respondents were asked what has kept or is most likely to keep organizations from moving their file data to the cloud.

Challenge	%
Security concerns	39%
File synchronization and collaboration between departments	27%
Ability to rapidly recover from a disaster or cyberattack	27%
Data classification/ compliance requirements	26%
Meeting application or user performance expectations	23%
Managing a fragmented data environment	21%
Overage costs associated with purchasing more storage	19%
Other	1%

1,000 respondents were asked what their biggest challenges are when managing file data infrastructure today.

Public sector is most concerned about data security

Of all industries surveyed, **the public sector is most concerned about security when it comes to file data management.**

More than half (52%) say it's the biggest challenge – perhaps unsurprising when we consider many bodies are managing highly sensitive data with underfunded or legacy systems.

Keeping data secure is the top concern (though to a lesser extent) for most sectors, but three have more pressing issues. The #1 challenge for financial services organizations is being able to quickly recover from disasters and cyberattacks. Energy, oil, and gas companies are most concerned about being able to synchronize files for collaboration, while media and advertising agencies struggle equally with storage costs and file synchronization.

#1 file data management challenge by sector

Security	52% Public sector	Quick recovery from disaster or attack	39% Financial services	File synchronization	30% Energy, oil, and gas	File synchronization and cost associated with buying storage	30% Media and advertising

When looking at what might prevent organizations from moving file data to the cloud, the picture is more straightforward. Security concerns come out top, across the board, with public sector (57%) being the most worried.

1,000 respondents were asked what their biggest challenges are when managing file data infrastructure today.

Section 3:
The impact of AI

Opportunities and roadblocks encountered on the AI implementation journey.

C-suite heavily involved in AI decision making

The importance of AI to business growth, competitiveness, and efficiency is underlined by the balance of decision making across organizations.

Once the preserve of technical teams, **decision making is now balanced fairly evenly between the IT department and the C-suite.**

39%
IT department

38%
C-suite executives

12%
Cross-functional team involving multiple departments

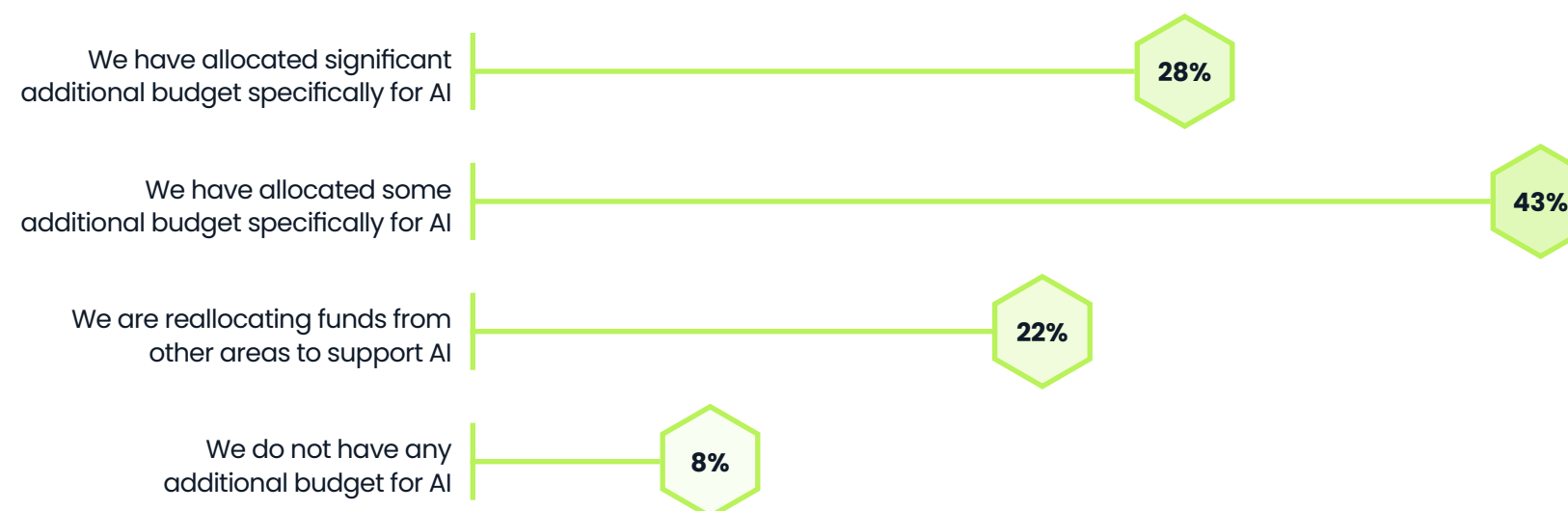**10%**
Data science or analytics department

Only 2% of organizations don't consider AI a priority

1,000 respondents were asked who holds the primary decision making authority regarding AI-related initiatives within their organization.

No matter how tight the budget, firms find money for AI

Despite the pressure on enterprise technology budgets, a whopping **92% of organizations have found budget for AI.**

Most (71%) have raised additional budget, but 22% are reallocating funds from other areas. In the race to capitalize on AI, non-AI-related projects across the business may find themselves needing to work harder to justify their own budgets.

We have allocated significant additional budget specifically for AI	28%
We have allocated some additional budget specifically for AI	43%
We are reallocating funds from other areas to support AI	22%
We do not have any additional budget for AI	8%

In the public sector, where securing extra funds is notoriously hard, organizations are most likely to have zero additional AI budget (21%), and also most likely (30%) to be reallocating money from elsewhere.

Media and advertising (51%) and financial services (42%) are the top sectors allocating significant extra budget to AI.

1,000 respondents were asked how they would describe their businesses approach to investment in AI initiatives.

AI is expected to deliver ROI – but measurement is a struggle

Firms may be allocating extra funds and shifting budget around to resource AI rollout, as they anticipate the investment will pay dividends.

The top expected outcome (46%) is cost reduction.

46%
Cost reduction/ savings

39%
Automation of certain workflows

36%
Enhanced customer experiences

33%
Advanced data management and visibility

25%
Faster content creation

1,000 respondents were asked what outcomes or return on investment (ROI) they aim to achieve by adopting AI solutions.

However, proving return on investment is another matter. **Organizations will need to manage, consolidate, and analyze their data accurately to prove the AI business case — and so far, less than a third are able to do so.**

We see variances across countries when it comes to the percentage of an organization's AI projects that are delivering accurately measurable ROI, with the DACH region leading the field.
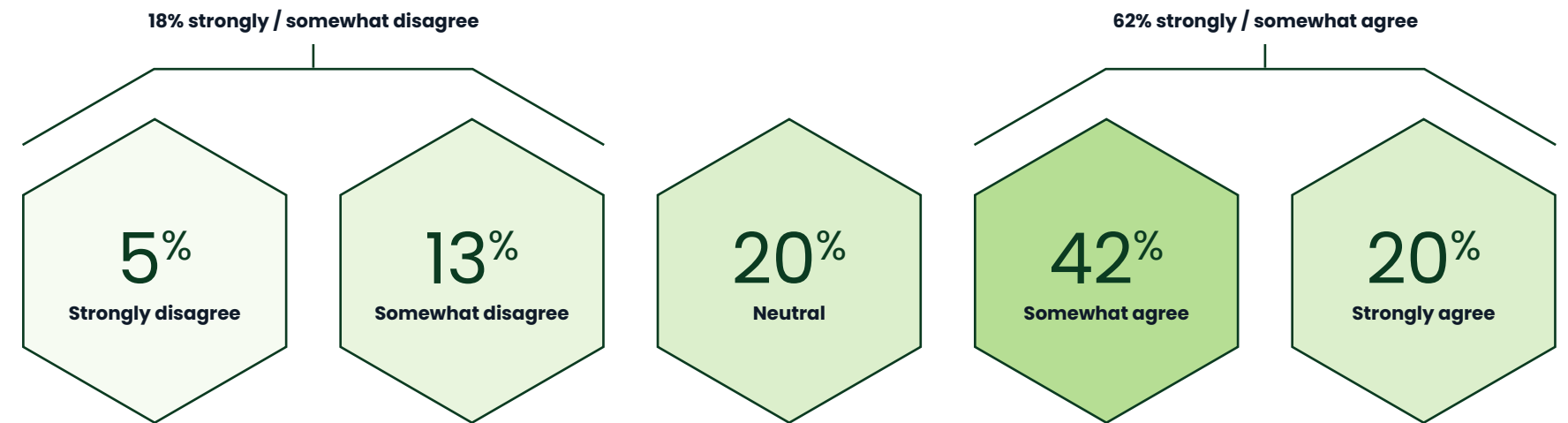
DACH 34%

US 27%

UK 26%

France 23%

1,000 respondents were asked what percentage of their organization's AI projects are delivering an accurately measurable ROI.

Globally, only 27% of AI projects are delivering an accurately measurable ROI

Only 1 in 5 are confident their data is AI-ready

Disorganized data and siloed working will hamper firms' AI ambitions.

Only 20% strongly agreed that their data is organized, accessible, and ready for AI initiatives.

18% strongly / somewhat disagree

62% strongly / somewhat agree

5%	13%	20%	42%	20%
Strongly disagree	Somewhat disagree	Neutral	Somewhat agree	Strongly agree

Company size plays a role – the larger the company, on the whole, the less likely the data is to be AI-ready. This makes sense in terms of the number of disparate teams, offices, and file locations where data may be held.

| 66%	58%	62%	59%	55%
1,000–4,999	5,000–9,999	10,000–24,999	25,000–50,000	50,000+

1,000 respondents were asked if they agreed with this statement: "My organization's data is structured, accessible, and ready for AI initiatives".

Firms spend more on cloud to support AI ambitions

On average, organizations are spending 18% more on the cloud to facilitate their AI initiatives.

The figure increases to 20% for AEC firms, 22% for financial services, and 30% for media and advertising. This trend can partly be attributed to the fact that many AI services are only available in the cloud, or via the major cloud providers.

Cloud spending has increased across the board, with even traditionally cash-strapped sectors like healthcare (14%) and public sector (11%) stepping up investment.

Mean:
18%

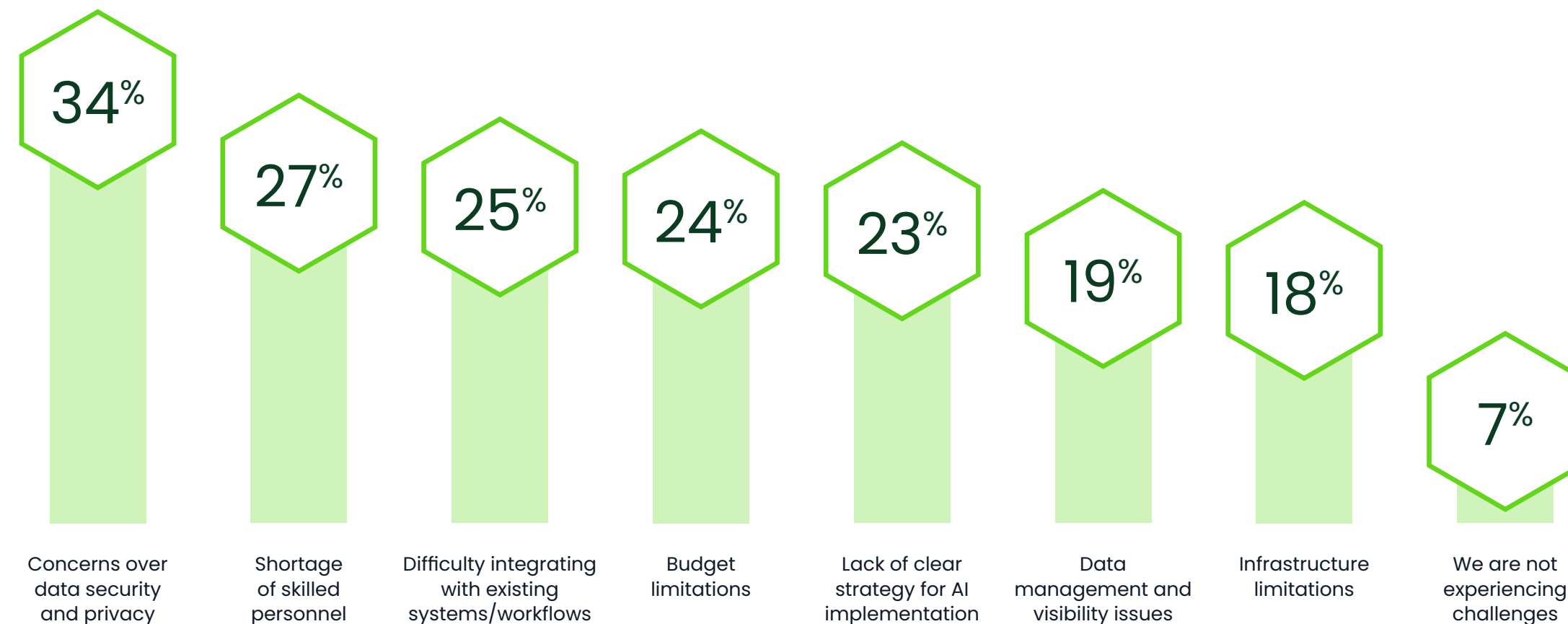| 9%	32%	39%	16%	4%
No increase	1% to 10%	11% to 25%	26% to 50%	Over 50%
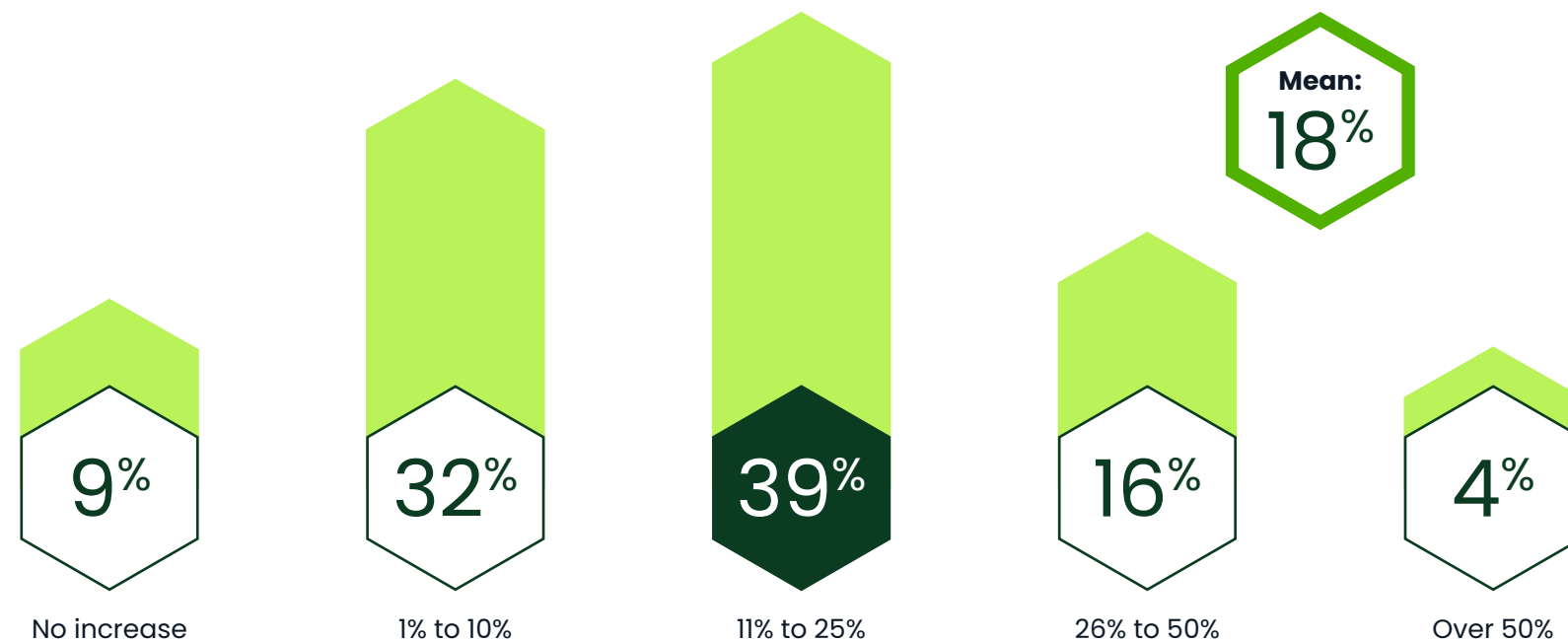
1,000 respondents were asked how much their AI initiatives have increased their organization's cloud spending.

Data security concerns and skills shortages hamper AI rollout

Despite the expected ROI from AI, and the budget being allocated, barriers to implementation still exist.

The security risks attendant on AI – or any new technology – aren't always fully understood: **over a third (34%) worry about data security and privacy.** A further 27% don't have the skills in-house to harness the technology's potential.

34%	27%	25%	24%	23%	19%	18%	7%
Concerns over data security and privacy	Shortage of skilled personnel	Difficulty integrating with existing systems/workflows	Budget limitations	Lack of clear strategy for AI implementation	Data management and visibility issues	Infrastructure limitations	We are not experiencing challenges

1,000 respondents were asked what the main challenges are when it comes to the implementation of AI initiatives in their organization.

Adopting a hybrid cloud model is an effective risk mitigation strategy

Organizations without plans to implement such a model are **more likely (51%)** to have data security and privacy concerns compared to those who are **already using a hybrid cloud model (31%).**

Section 4:
Storage and cybersecurity

Top concerns in the battle to protect companies' valuable assets from cybercriminals.

Firms are overconfident in ability to recover from attacks

Global ransomware payments have declined from a record $1.25bn in 2023[4], which is good news for everyone.

However, the 2024 total of $813m is still significant – and when you add in the reputational damage and commercial impact of downtime from cyberattacks, they represent a major problem.

It's a problem some organizations aren't fully aware they have, because of misplaced confidence in their cybersecurity preparedness. **63% say they feel confident their organization can recover critical unstructured data and cope with a destructive cyberattack.** And yet, over the past year, 69% experienced an attack, and **45% suffered a breach which resulted in either a ransom payment, costly downtime, data loss, reputational damage, or issues recovering data.**

4   www.theguardian.com/technology/2025/feb/05/global-ransomware-payments-plunge-by-a-third-amid-crackdown
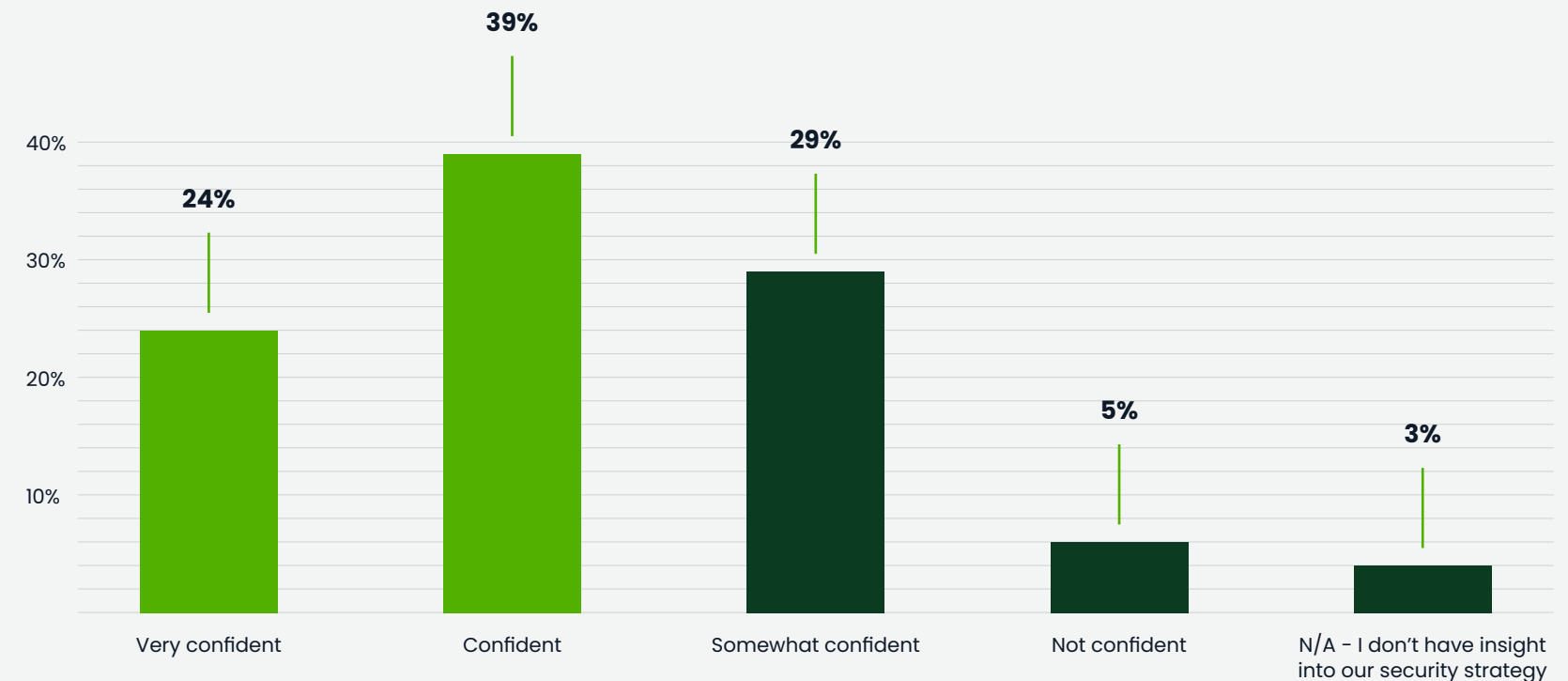
1,000 respondents were asked how confident they are in their organization's ability to recover critical unstructured data and cope with a destructive cyberattack.
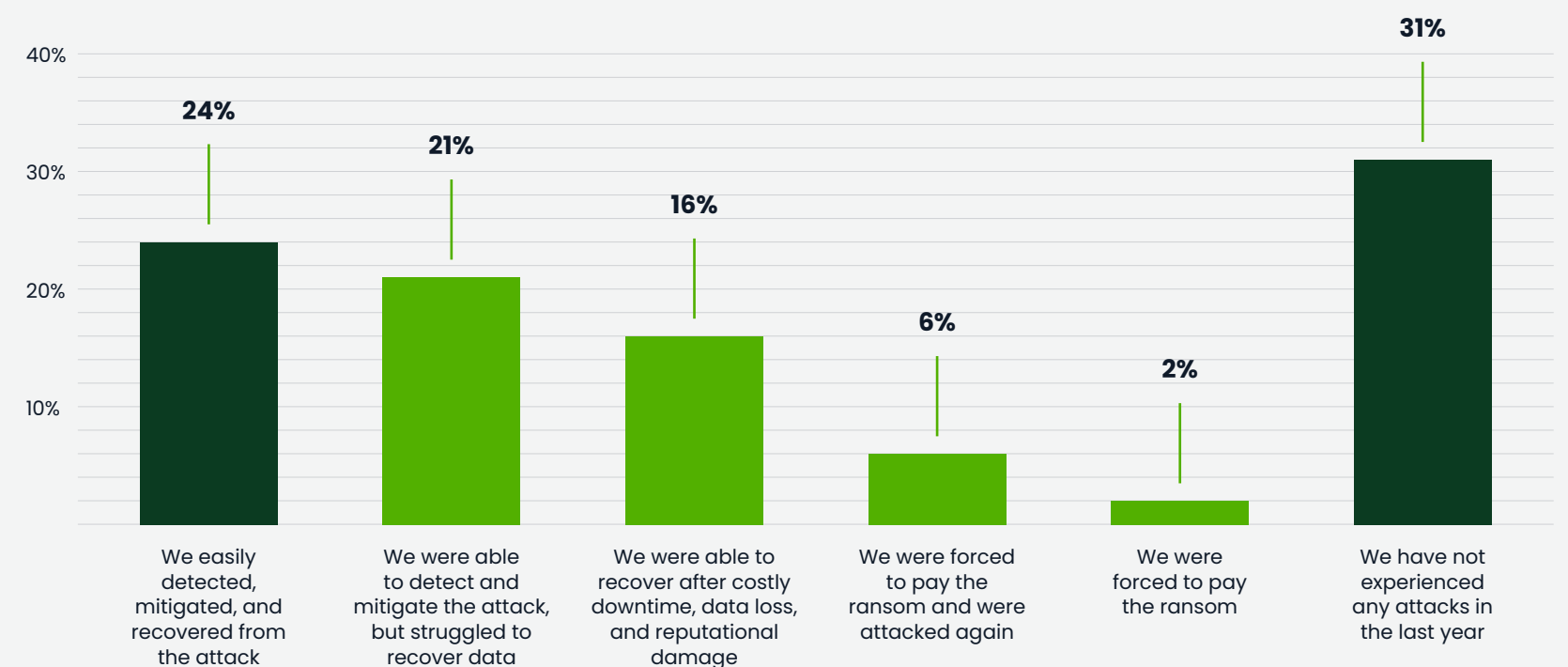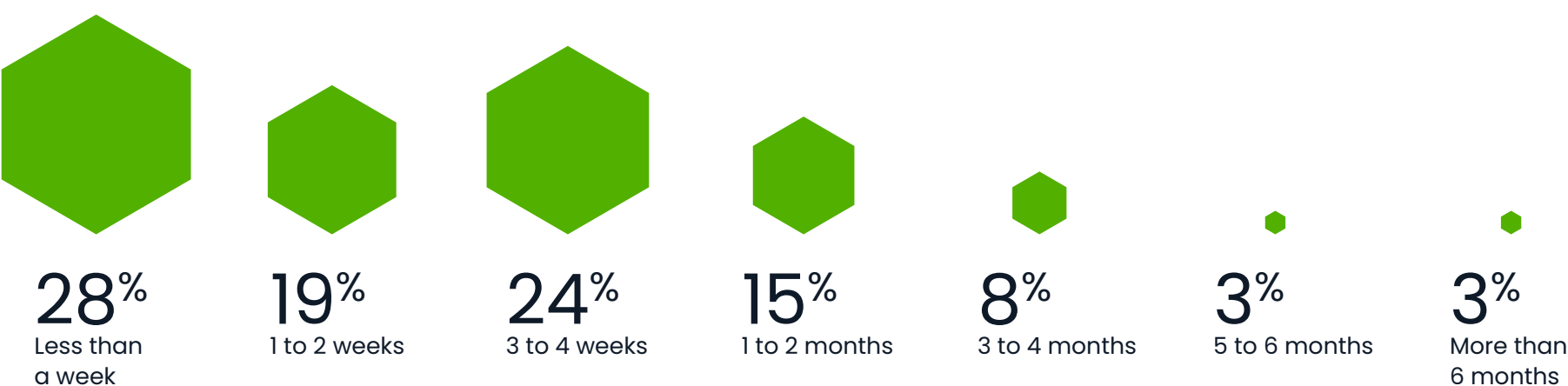

1,000 respondents were asked what the main outcome was of any cyberattacks experienced in the last year.

Five weeks needed to recover from cyberattacks

On average, it took organizations five weeks to get back to normal after their most recent cyberattack.

72% took more than a week to recover. When you consider the average cost of downtime is calculated to be around $300,000 per hour[5], that equates to at least $50m lost per incident.

28%
Less than a week

19%
1 to 2 weeks

24%
3 to 4 weeks

15%
1 to 2 months

8%
3 to 4 months

3%
5 to 6 months

3%
More than 6 months

1,000 respondents were asked how long it took their organization to fully recover the last time it experienced a cyberattack.

Disruption was shown to be shorter-lived for those with a hybrid cloud infrastructure, who were more likely to take less than a week to recover (29%) than those without (23%).

---

5 www.vertiv.com/globalassets/documents/reports/2016-cost-of-data-center-outages-11-11_51190_1.pdf

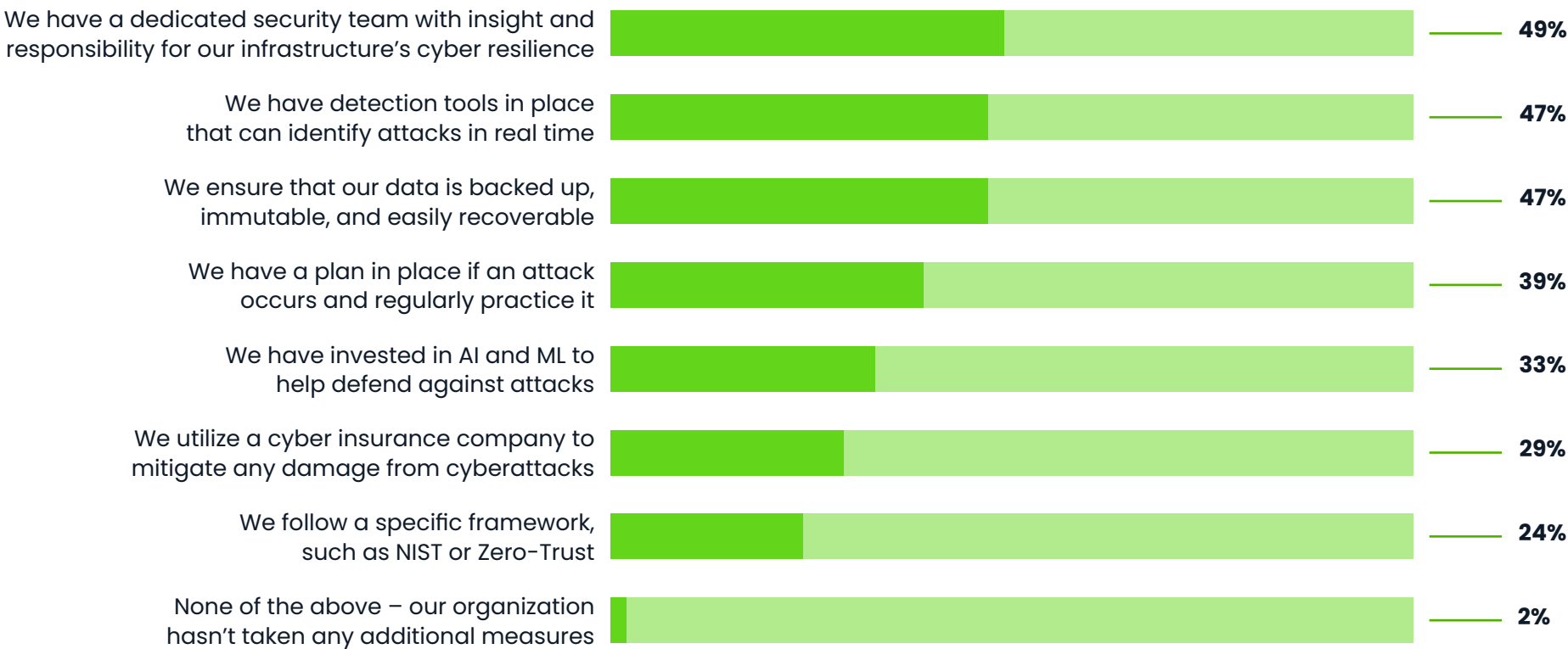# Which sectors take longest to recover?

Despite 66% of **manufacturing** firms feeling confident in coping with a destructive cyberattack, they take a higher than average 6.3 weeks to recover, and 50% have suffered an attack which resulted in either a ransom payment, costly downtime, data loss, reputational damage, or issues recovering the data.

Healthcare and life sciences organizations need just over 6 weeks to recover from an attack. 47% have suffered an attack which resulted in either a ransom payment, costly downtime, data loss, reputational damage, or issues recovering the data.

Room for improvement in cyber resilience measures

Given the timeframes and costs involved in recovering from cyberattacks, the number of firms without basic measures in place is surprising.

More than half (53%) don't have detection tools in place to identify attacks in real time. A further 53% say their data isn't backed up, immutable, and easily recoverable.

Measure	Percentage
We have a dedicated security team with insight and responsibility for our infrastructure's cyber resilience	49%
We have detection tools in place that can identify attacks in real time	47%
We ensure that our data is backed up, immutable, and easily recoverable	47%
We have a plan in place if an attack occurs and regularly practice it	39%
We have invested in AI and ML to help defend against attacks	33%
We utilize a cyber insurance company to mitigate any damage from cyberattacks	29%
We follow a specific framework, such as NIST or Zero-Trust	24%
None of the above – our organization hasn't taken any additional measures	2%

Organizations need to test the validity of their readiness beliefs alongside their actual cybersecurity measures.

Just 44% of **financial services** firms say their data is backed up, immutable, and easily recoverable – despite the fact that 70% say they're confident in their ability to recover unstructured data.

Meanwhile the **public sector**, with only 45% confidence in being able to recover data after an attack, are more likely (53%) to say their data is backed up and easily recoverable.

1,000 respondents were asked measures their organization has taken to make their data more cyber resilient.

Key takeaways

Organizations are taking steps to protect their file data, prepare it for AI, and make it accessible for efficient collaboration. Those who rely on legacy, on-premise storage solutions will struggle to compete in the era of hybrid cloud.

Make sure your resilience reality matches perception

There's a mismatch between how quickly and effectively organizations believe they can recover data after a cyberattack, and the reality.

When firms are taking five weeks on average to get back to normal, that's a huge cost to the company. Choosing a hybrid cloud storage solution with integrated disaster recovery and ransomware protection limits the impact of breaches.

Help teams work more efficiently

The second biggest challenge posed by managing file infrastructure (after security) is file synchronization, to help different teams collaborate effectively.

Nasuni's intelligent edge cache, for both on-premises and cloud, offers quick read/write access to active files, and dynamic synchronization across all locations.
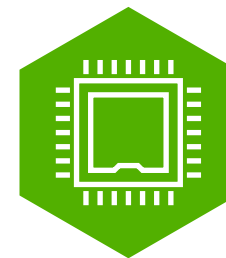
Create an environment that supports AI

Almost all firms (98%) say AI is a priority. In that case, the same number should be prioritizing hybrid cloud file data storage – because AI initiatives can't succeed if data is poorly structured, lost, or inaccessible.

At Nasuni, our clients fuel their AI projects with consolidated, unified data across cloud and on-premises, via a single pane of glass.

> Organizations are making AI a top priority and significantly ramping up their investments, but what we are finding is they are not always taking the critical steps necessary to ensure success when it comes to data management.
>
> A modern approach that unifies, organizes, and makes unstructured data accessible is needed to reliably and securely harness AI, enabling teams to navigate the complexities of AI deployment confidently.

David Grant, President at Nasuni

About Nasuni

Nasuni **is a unified file data platform for enterprises facing an explosion of unstructured data, combining storage and data services into a single hybrid cloud solution.**

Nasuni's approach enables business resiliency and better data management, while providing solutions that drive IT efficiency – cutting infrastructure costs by up to 67%. Its best-in-class solution also eliminates the need for additional cybersecurity measures or separate backup and disaster recovery. The Nasuni File Data Platform replaces the friction associated with legacy infrastructure with optimized infrastructure flow, supporting modern enterprise expectations for data analytics and business insights.

Nasuni helps businesses transform data from an obstacle into an opportunity. Organizations worldwide rely on Nasuni, spanning the manufacturing, media and advertising, construction (AEC), consumer brands, and energy industries. Its corporate headquarters are located in Boston, Massachusetts, and the company delivers services to over 70 countries. For more information, visit **nasuni.com.**

About Sapio Research

Sapio Research **is a full-service B2B and tech market research agency that helps businesses grow thanks to high quality, efficient and honest research solutions.**

We deliver valuable insights to support our clients understand their audience, build powerful brands, cut through the noise with great content and thought leadership. We're based in the UK and have access to over 149 million people across 130 countries, working with clients that range from top tech companies to global consultancies, Marketing/PR agencies and household name brands.

Our purpose-driven team of expert market researchers is passionate about providing data confidence for all and performing research that makes a difference. We're here to support our clients every step of the way in all areas of quantitative and qualitative research, so they can save time and thinking space, deliver with confidence, and unlock more value with their research. For more information, visit **sapioresearch.com**.

≡ NASUNI