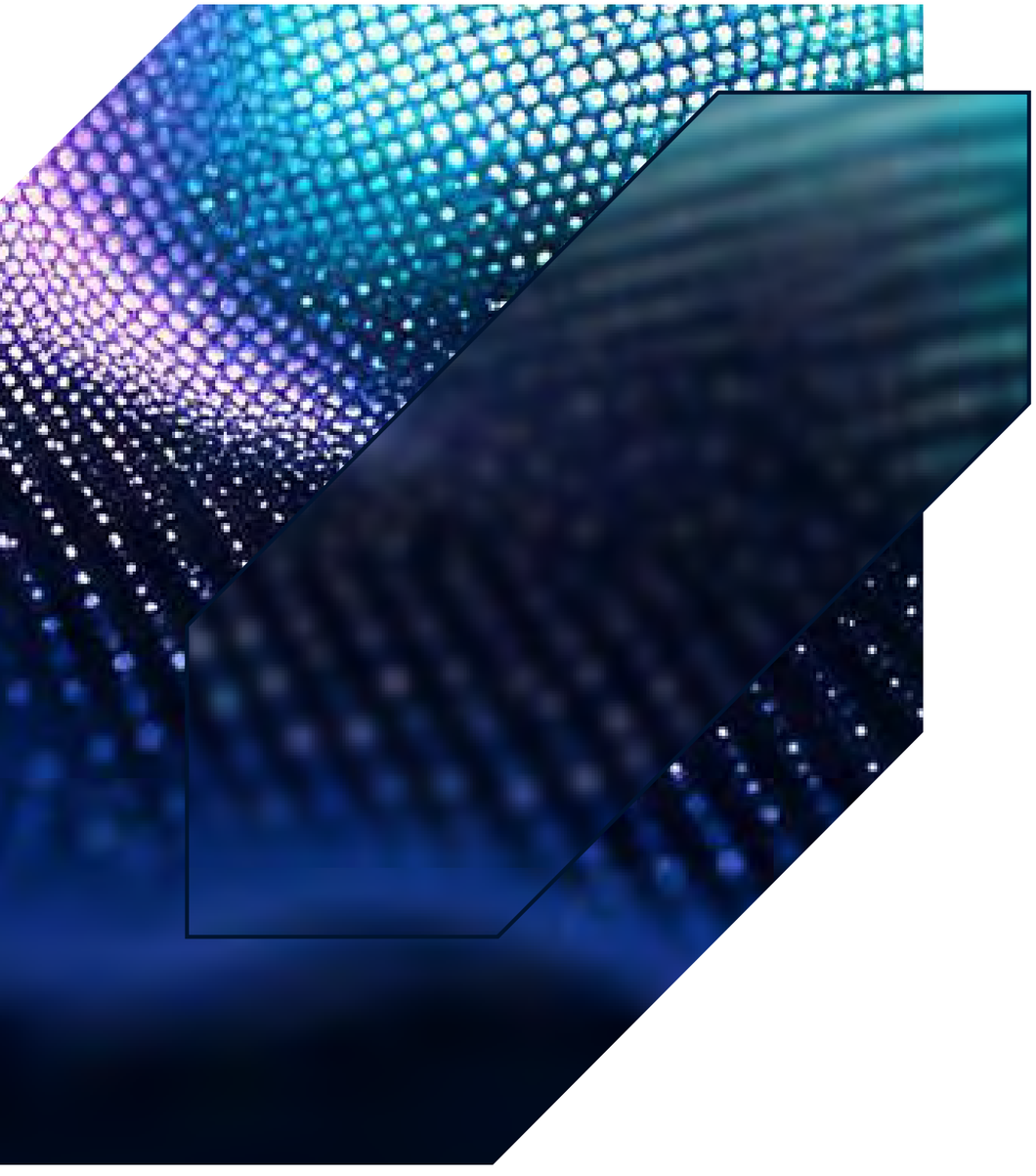
II:II SYSTEMS

2027 State of IT Infrastructure Resilience

ANZ Edition



THE RESILIENT CLOUD PLATFORM



For ANZ organisations, resilience is becoming an infrastructure coordination challenge.

11:11 Systems' 2027 State of IT Infrastructure Resilience survey shows that Australia and New Zealand IT leaders are making infrastructure and budget decisions with two big worries in mind: infrastructure costs keep climbing and cyber threats aren't going away. Identity platforms and production environments top the list of leading data centre concerns in the region, while hybrid complexity and inconsistent data protection make it difficult to maintain a reliable recovery plan.

AI adds another layer of urgency. Nearly all ANZ respondents are either investing in or evaluating AI-enhanced IT and security tools, but fewer than one in five report that AI-enhanced backup or disaster recovery is operational today. There's a clear gap between AI ambition and recovery readiness, and it tells us something important: focus investment on capabilities that make resilience easier to see, test, and put into action.

93% 93% of ANZ respondents report that their data centre infrastructure costs increased over the past 12 months.

61% 61% use three or more backup products across their production platforms.

93% 93% are embracing AI in their IT and security operations, with 63% who are actively investing in AI and 30% who are evaluating AI options.

The 2027 State of IT Infrastructure Resilience eBook explores how to simplify complex environments, protect the systems designed to restore the business, and turn AI investment into practical improvements in detection, validation, and recovery.

Keep reading our 2027 State of IT Infrastructure Resilience eBook to understand the global challenges and priorities shaping the industry.

© 2026 11:11 Systems. All rights reserved.

TABLE OF CONTENTS

Executive Summary 04

Methodology 06

Key finding #1 07
Shift in strategic decision sets

Key finding #2 08
Barriers in complexity

Key finding #3 09
Impact of AI urgency

Key finding #4 10
Cyber recovery and operational resilience

Key finding #5 11
Key organisational vulnerabilities

Conclusion 12

Resources 13

© 2026 11:11 Systems. All rights reserved.

EXECUTIVE SUMMARY

A new reality demands a new approach.

Information Technology is at an inflection point. Current cost pressures, platform changes, the rise of artificial intelligence (AI), and ongoing security concerns are no longer separate conversations. They're converging into a single, high-stakes challenge for IT leaders. At 11:11 Systems, we refer to this as the Great Infrastructure Reset.

CONVERGING FORCES

Cost pressures

Platform changes and the rise of AI

Ongoing security concerns

A more complex landscape

Organisations are managing more than ever before.

- More distributed systems
- Growing dependencies
- Increasing volumes of data

Organisations are managing more distributed systems, dependencies, and data than ever before. Meanwhile, the evolution of service expectations for technology architecture and delivery models is happening at an ever-increasing pace. But how are organisations managing this monumental change?

11:11 Systems recently conducted a research study of more than 700 IT professionals across a range of global geographies and industries.
We uncovered several themes supporting a central argument: resilience is no longer a technology question alone. It is a strategic business imperative.

© 2026 11:11 Systems. All rights reserved.

OVERVIEW

Five Key Global Findings

In this age of the Great Infrastructure Reset, understanding the changes affecting IT, infrastructure, and operational resilience is critical.

Whether you're a C-level executive, line-of-business leader, or on the frontlines of technology, having a clear view of the current shift and its effect on resilience is an urgent requirement.

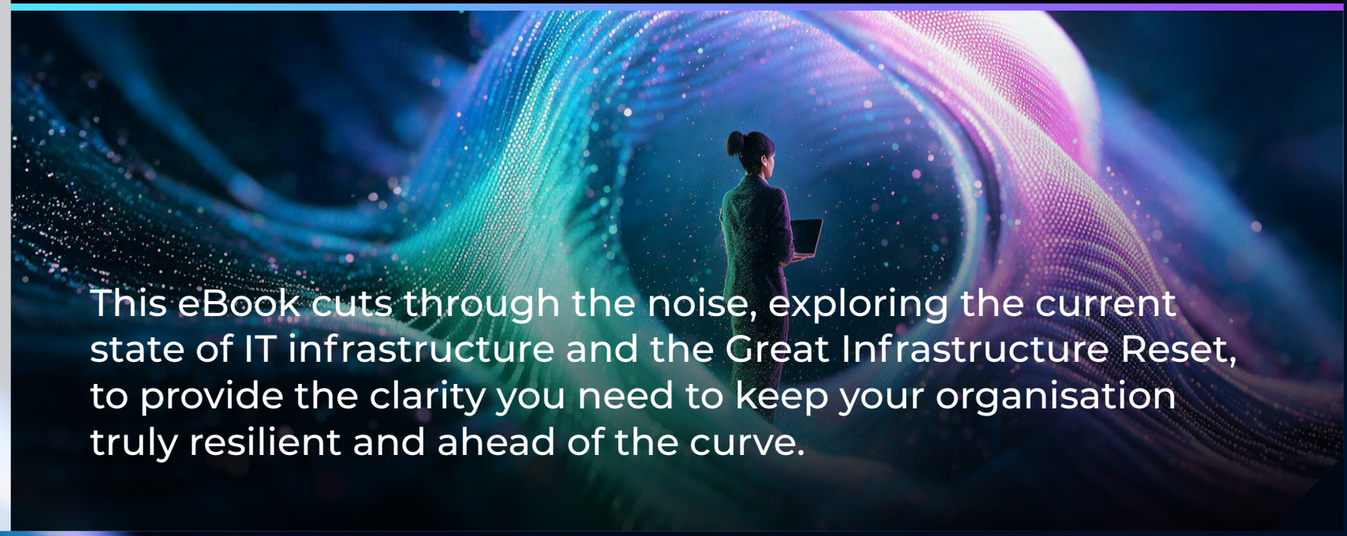
To navigate this reset effectively, it's essential to first establish what resilience truly means in our complex IT landscape. For the purposes of this eBook, IT infrastructure resilience is an organisation's ability to anticipate disruption, overcome its effects, adjust operations, and restore or maintain critical services while protecting business priorities.

It goes beyond backup, disaster recovery, and business continuity planning to emphasise preparedness, adaptability, continuous improvement, and operating through uncertainty—across the full IT stack.

Building on our initial research from the 11:11 Cyber Trends Report, this year's study uncovered even greater concern about operational resilience in the face of increasing pressure.

Five themes emerged from the data:

1. Complexity remains the primary barrier to resilience, not budget or talent alone.
2. AI interest is high, but operational deployment lags behind expectation.
3. Cyber recovery has evolved from a backup concern into a core operational resilience issue.
4. Organisations are increasing IT investments, yet key vulnerabilities persist.
5. The decisions organisations make today will define their competitive position for years to come.



This eBook cuts through the noise, exploring the current state of IT infrastructure and the Great Infrastructure Reset, to provide the clarity you need to keep your organisation truly resilient and ahead of the curve.

© 2026 11:11 Systems. All rights reserved.

Methodology

In 2026, we surveyed **734 IT leaders at organisations** ranging from 250 to more than 5,000 employees.

Respondents were all directly involved in IT infrastructure, cybersecurity, or backup/disaster recovery (DR) roles in their organisations. We surveyed people in a variety of industries, including Manufacturing, Financial Services, Retail, Healthcare, Government, Education, Energy, Transportation, and more.

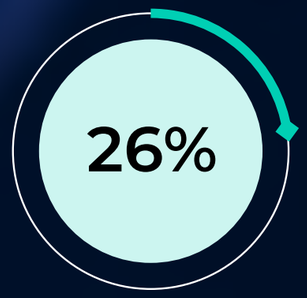
The global survey included respondents from seven countries across EMEA, the Americas, and APAC.

11:11 Systems, in partnership with Veeam, commissioned Data Protection Matters (DPM) to conduct this research. DPM is an independent analyst firm covering data protection, cyber resilience, business continuity and disaster recovery (BC/DR), and BaaS/DRaaS. DPM conducts primary market research and develops content to help leaders separate marketing hype from the technologies and practices that actually matter for IT resilience.

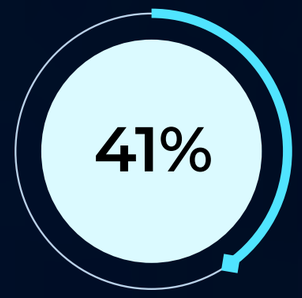
The study was designed and analysed by DPM Principal Analyst & Founder Jason Buffington, who brings 35 years of data protection, BC/DR, and cyber resilience experience to DPM's coverage.



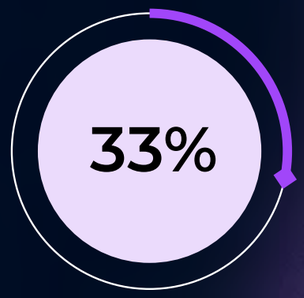
Data Protection Matters



Midmarket
(250-999 employees)



Enterprise
(1,000 – 5,000 employees)



Large Enterprise
(more than 5,000 employees)

veeam

© 2026 11:11 Systems. All rights reserved.

Key finding #1

Shift in strategic decision sets

Cost pressure, platform change, and security concerns are converging into one strategic decision set.

Infrastructure strategy is more complex than ever.

Our survey found that IT leaders are no longer just thinking about performance or technology. They're also factoring in costs, cybersecurity, licensing, cloud economics, and integration together.

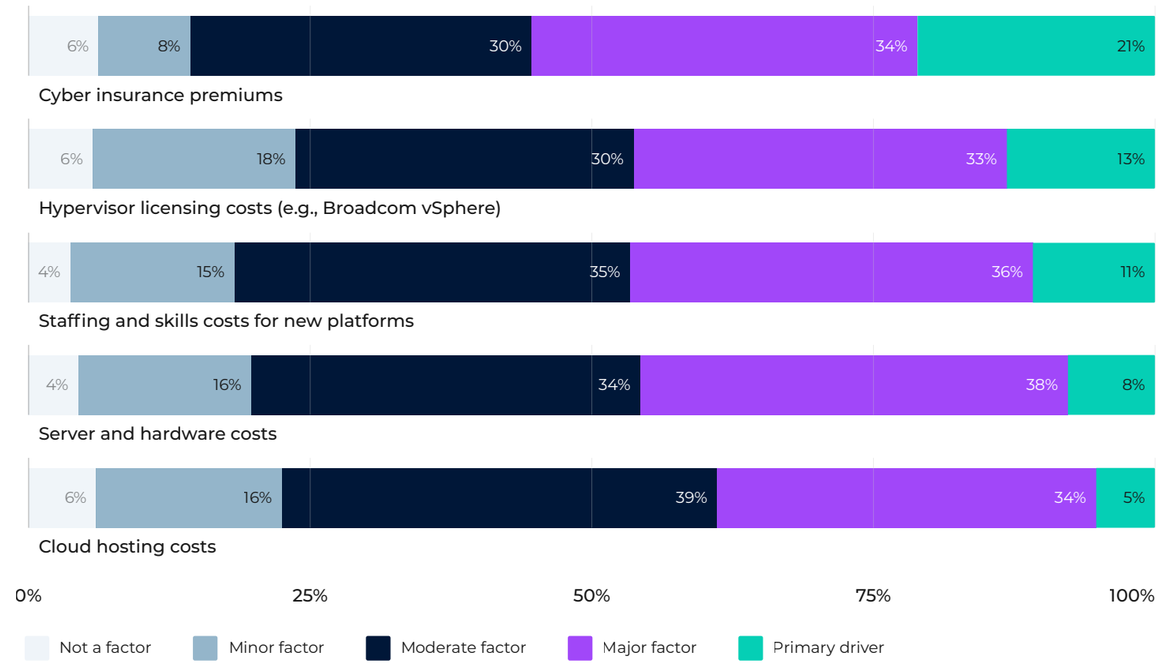
- 90% of respondents say their data centre infrastructure costs increased over the past 12 months.
- When evaluating 2027 infrastructure strategy, server and hardware costs are a major factor or primary driver for 46% of respondents.
- Among respondents making vSphere decisions for 2027, cybersecurity and integration requirements are the primary driver (50%) followed by licensing costs, network costs, and existing teams' skills.
- Cyberattacks on production platforms are the top data centre strategy concern for 43% of respondents.

What this means

Choosing the right infrastructure isn't about deciding whether to stay on-premises, migrate to the cloud, or do both.

Particularly in the age of The Great Infrastructure Reset, it's about building a model that can handle rising costs while keeping your infrastructure and data secure, your systems connected, and your business recoverable when things go wrong. Increasingly, platform choices are resilience choices.

When evaluating changes to your IT infrastructure strategy for 2027, how significant a factor is each of the following cost pressures?



© 2026 11:11 Systems. All rights reserved.

Key finding #2

Barriers in complexity

Complexity is still the primary barrier for resilience, not simply budget or talent.

Organisations don't lack the will to recover.

They just don't have the simple tools to do it. The survey reveals that most organisations are juggling many platforms, systems, and backup products, all of which require different skills to manage, and makes IT even more complex.

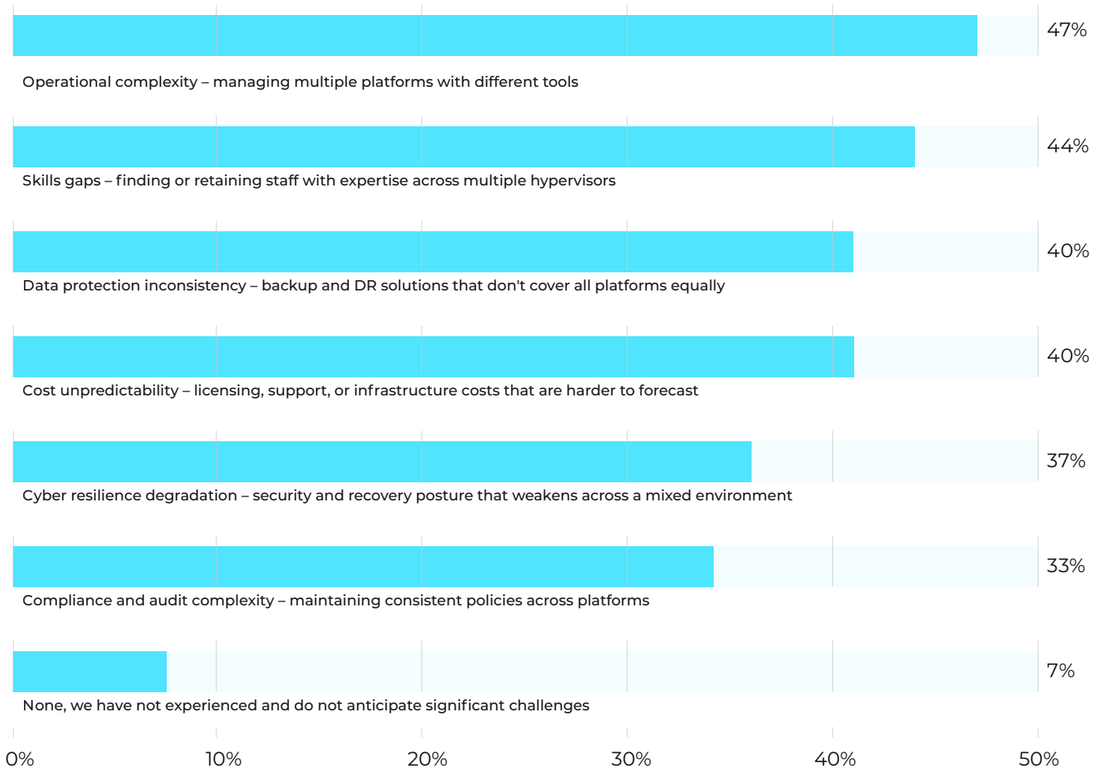
- 56% identify the complexity of planning required for cyber incident recovery as their biggest challenge.
- Across multiple hypervisors or hybrid cloud environments, 47% cite operational complexity, 44% cite skills gaps, 40% cite cost unpredictability, and 40% cite inconsistent data protection across platforms.
- 87% of respondents use two or more backup products across their production platforms.
- Among respondents running multiple hypervisors or hyperscale hosts, the leading challenges include different cybersecurity capabilities across platforms at 40%, multiple management consoles at 36%, and complexity of VM operations at 34%.

What this means

Complexity is a system-level problem—and a direct challenge to operational and cyber resilience. Even with the right budget, team, and tools, businesses can still struggle with data protection when those tools don't work well together.

The data shows that how well your tools integrate and coordinate is just as important as how good each individual tool is.

Thinking about managing servers across multiple hypervisors and/or hybrid cloud environments, which of the following challenges have you experienced or anticipate facing?



Note: Respondents were able to list up to three challenges, so totals will not equal 100%.

© 2026 11:11 Systems. All rights reserved.

Key finding #3

Impact of AI urgency

AI urgency exceeds AI readiness.

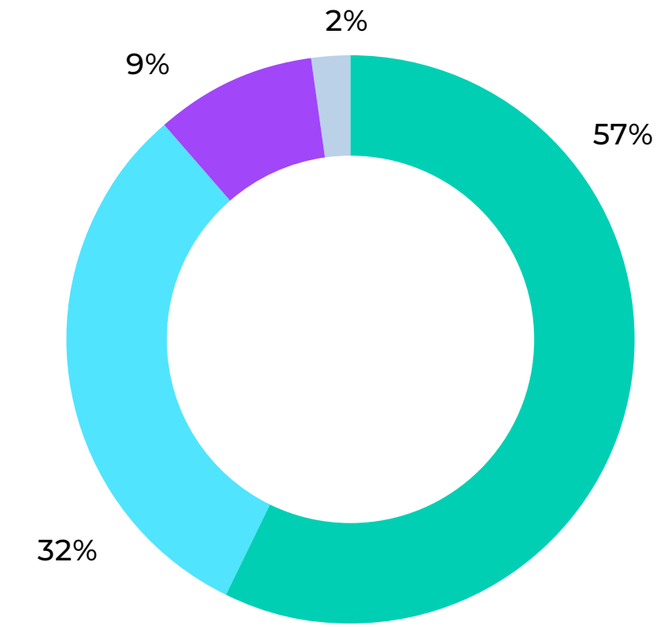
AI is a priority for IT and security teams, particularly in the age of The Great Infrastructure Reset. But while many businesses are investing in it (or plan to), most aren't ready to use it effectively, especially when it comes to backup and DR. Across respondents:

- 57% say they are actively investing in AI-enhanced IT or security tools, while another 32% are evaluating AI tools but have not yet committed budget.
- 78% are at least somewhat concerned that AI-accelerated malware or ransomware will make attacks more sophisticated or frequent.
- Only 19% report that AI-enhanced backup or DR capabilities are operational today.
- The most sought-after AI capability in backup and DR is detecting cyber anomalies during protection, selected by 58% of respondents.

What this means

AI is reshaping the security landscape, with frontier models such as Anthropic's Mythos demonstrating how vulnerabilities can be exploited at scale, and in record time. For backup and DR, the practical imperative is clear: use AI to detect threats early, validate recovery points, and simplify recovery. Broadcom (VMware's parent company) is helping lead this shift and working directly with Anthropic to harden its platform.

Thinking about AI in the context of your IT and security strategy for 2027, which of the following best describes your organisation's current position?



© 2026 11:11 Systems. All rights reserved.

Key finding #4

Cyber recovery and operational resilience

Cyber recovery is now an operational resilience issue, not just a backup issue.

The survey shows that cyber incidents can disrupt every part of your business, not just systems and data. Backups are important to your day-to-day operations. But having a backup doesn't always mean you can recover.

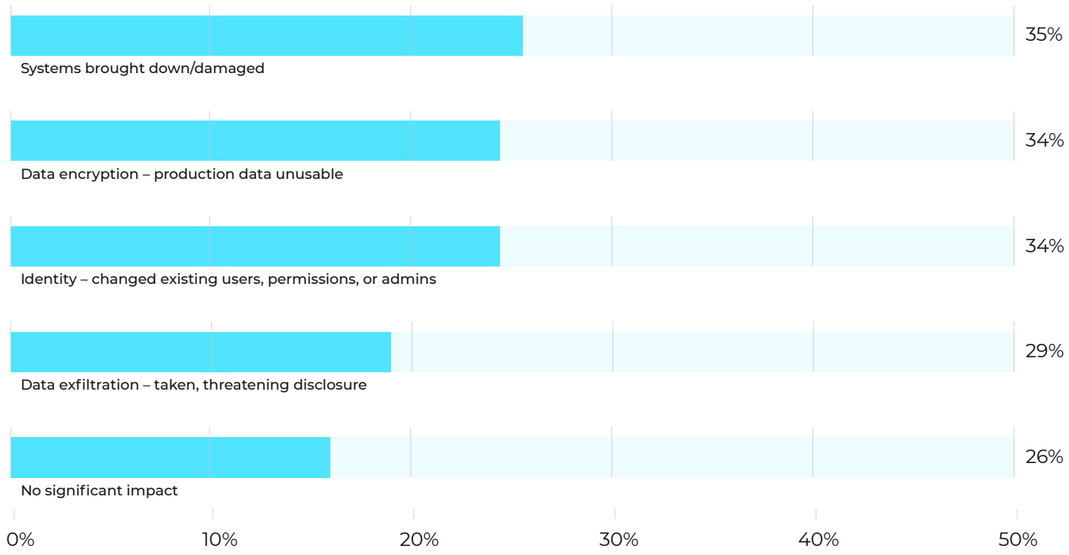
- Among respondents reporting cyberattack or breach impacts, 35% experienced systems being brought down or damaged, 34% experienced production data encryption that made it unusable, 34% experienced changes to existing users, permissions, or administrators, and 29% experienced data exfiltration.
- When systems or data were brought down, 81% restored data or systems from backup.
- 41% say that at least some of their backup repositories were affected during a cyberattack, and effectively 13% of their data was not recoverable.
- The leading driver for new cyber incident recovery solutions is improved data security and protection at 65%.

What this means

A good recovery strategy is more than just restoring data.

It also needs to include identity integrity, clean room recovery environments, failover decisions, monitoring, and regular testing. It should also assume that your data protection systems could be targeted. Cyber recovery is now a core part of business continuity planning.

Collectively, what kinds of impacts has your organisation experienced from cyberattacks or breaches?



Note: Respondents were able to list up to three challenges, so totals will not equal 100%.

© 2026 11:11 Systems. All rights reserved.

Key finding #5

Key organisational vulnerabilities

Organisations are investing aggressively, but key vulnerabilities remain.

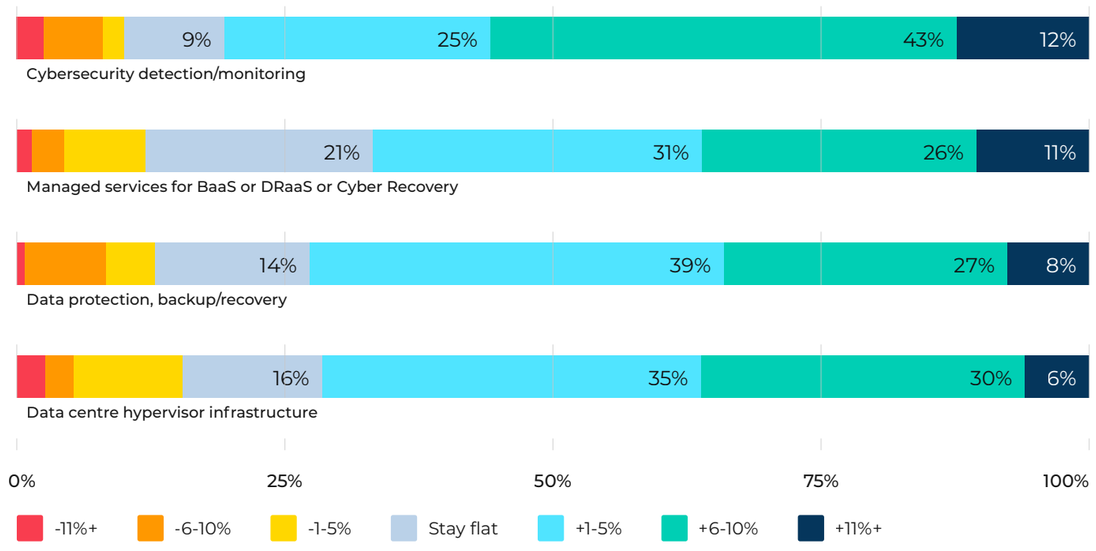
The survey shows more businesses are taking cyber threats seriously and investing in prevention. However, having a plan and a budget doesn't mean you can recover from an attack quickly or completely.

- 73% of respondents expect budgets for data protection, backup, and recovery to increase in 2027. Budget increases are also expected for managed services for BaaS, DRaaS, or cyber recovery at 67%, cybersecurity detection and monitoring at 81%, and data centre hypervisor infrastructure at 72%.
- 80% say they will definitely or probably consider new cyber resilience solutions, including backup or disaster recovery, for 2027.
- Nearly half of respondents, 49%, report that their systems were affected for two to five days.
- 43% of respondents estimated an hour of downtime cost their organisation between 251,000-1,000,000 USD.

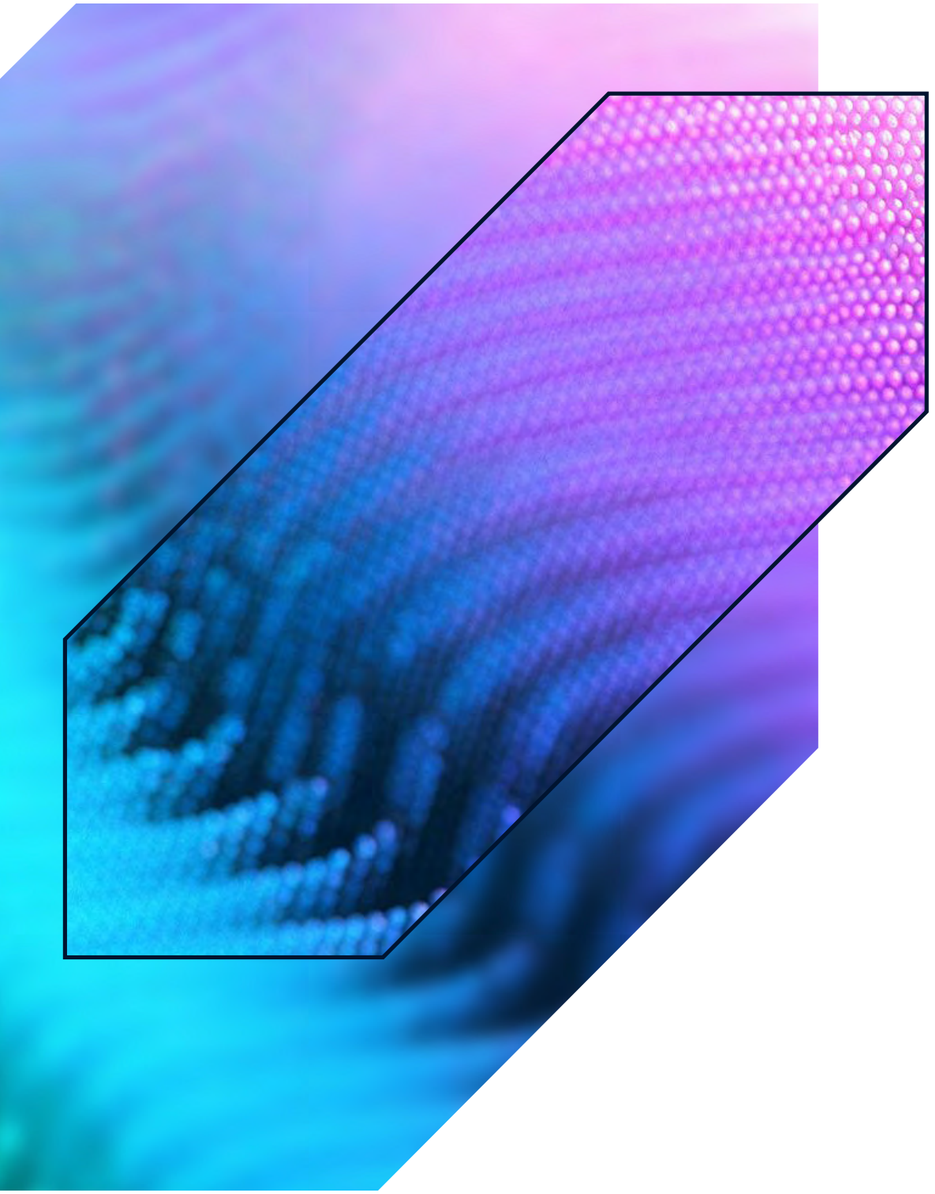
What this means

More organisations are investing in recovery plans, but that doesn't mean they're fully prepared. Many still struggle with corrupted backups, lengthy outages, and limited understanding of what downtime actually costs them. Having a plan is a good start, but the real measure of preparedness is whether that plan has been tested and can deliver reliable, cost-effective results when it matters most.

How do you expect budgets to shift for 2027?



© 2026 11:11 Systems. All rights reserved.



Conclusion

The 2027 IT environment will reward organisations that can reduce friction between strategy and execution. While this is easier said than done, the window for reactive planning is closing quickly. Largely due to The Great Infrastructure Reset, businesses must prioritise these initiatives in their 2027 planning, or they will risk increased costs, in addition to lagging behind the competition.

11:11 Systems' 2027 State of IT Infrastructure Resilience survey results highlight these imperatives and what organisations should do to assess their current resilience posture:

Simplify the operating environment where possible.

Reduce complexity and eliminate redundant infrastructure to improve efficiency across the board. This makes it easier to onboard new staff, troubleshoot issues, and scale quickly.

Treat infrastructure, security, backup, and recovery as connected decisions.

Platform reviews should include recovery dependencies and operational requirements, not just performance, capacity, and cost. By eliminating the inefficiencies of managing three separate work streams, enterprise IT organisations will streamline investments and drive smarter budget allocation.

Turn AI curiosity into real, measurable use cases.

By and large, businesses are making major investments in AI, but their operational maturity—including IT infrastructure, security, and processes—needs to develop as they implement programs.

Test recovery across the full IT stack, not just your backup, cyber recovery, or DR systems.

Your recovery plan is only as strong as the environment it operates in. A good testing program demonstrates the business can recover safely—and in the right sequence.

Base your resilience investments on your real cost of downtime and how quickly you can recover from disruptions.

Most organisations indicate they're planning to invest in recovery and cyber resilience solutions, but most don't yet have reliable figures on what downtime costs the business. Connect resilience investments with the solutions that will reduce the impact of unresolved gaps.

© 2026 11:11 Systems. All rights reserved.

The organisations best positioned for 2027 will not necessarily be those with the most tools. They will be those that can coordinate everything to recover cleanly.

This means aligning people, platforms, tools, processes, and decisions, even under pressure.

THE RESILIENT CLOUD PLATFORM

MODERNISE PROTECT MANAGE

1111systems.com



Resources

11:11 Cyber Trends Report

The Great Infrastructure Reset eBook

Great Infrastructure Reset Webinar

Ransomware Report

11:11 Systems, the 11:11 Systems logo, and all other 11:11 Systems product or service names are registered trademarks or trademarks of 11:11 Systems, Inc.
All other registered trademarks or trademarks belong to their respective owners. © 2026 11:11 Systems. All rights reserved.

veeam

11:11 SYSTEMS