Data Health Check

2026

Databarracks

EXECUTIVE SUMMARY

The Databarracks Data Health Check provides an annual snapshot of IT resilience in the UK, having tracked how organisations prepare for and respond to disruption since 2008.

The 2026 report shows organisations preparing for a harsher resilience environment, where serious cyber disruption is no longer treated as a remote possibility.

Following a year of high-profile cyber attacks across the UK, **65% of organisations now believe a serious cyber attack could threaten their survival**.

This concern is grounded in operational reality. **Cyber is the leading cause of downtime** for the fourth year in succession, with 30% of organisations citing it as their biggest cause of downtime. Cyber attacks and internal security breaches are also the leading combined cause of data loss, affecting 43% of organisations.

The full scale of cyber disruption may not be visible, however. **1 in 5 organisations say they have chosen not to report a serious cyber incident** to avoid negative consequences.

AI is accelerating the pressure. **AI-driven attacks have more than doubled in frequency over the last 12 months**, now affecting 25% of organisations. Despite this, **79% believe AI is a greater benefit than threat to security**, and 93% of resilience teams now use AI in some form.

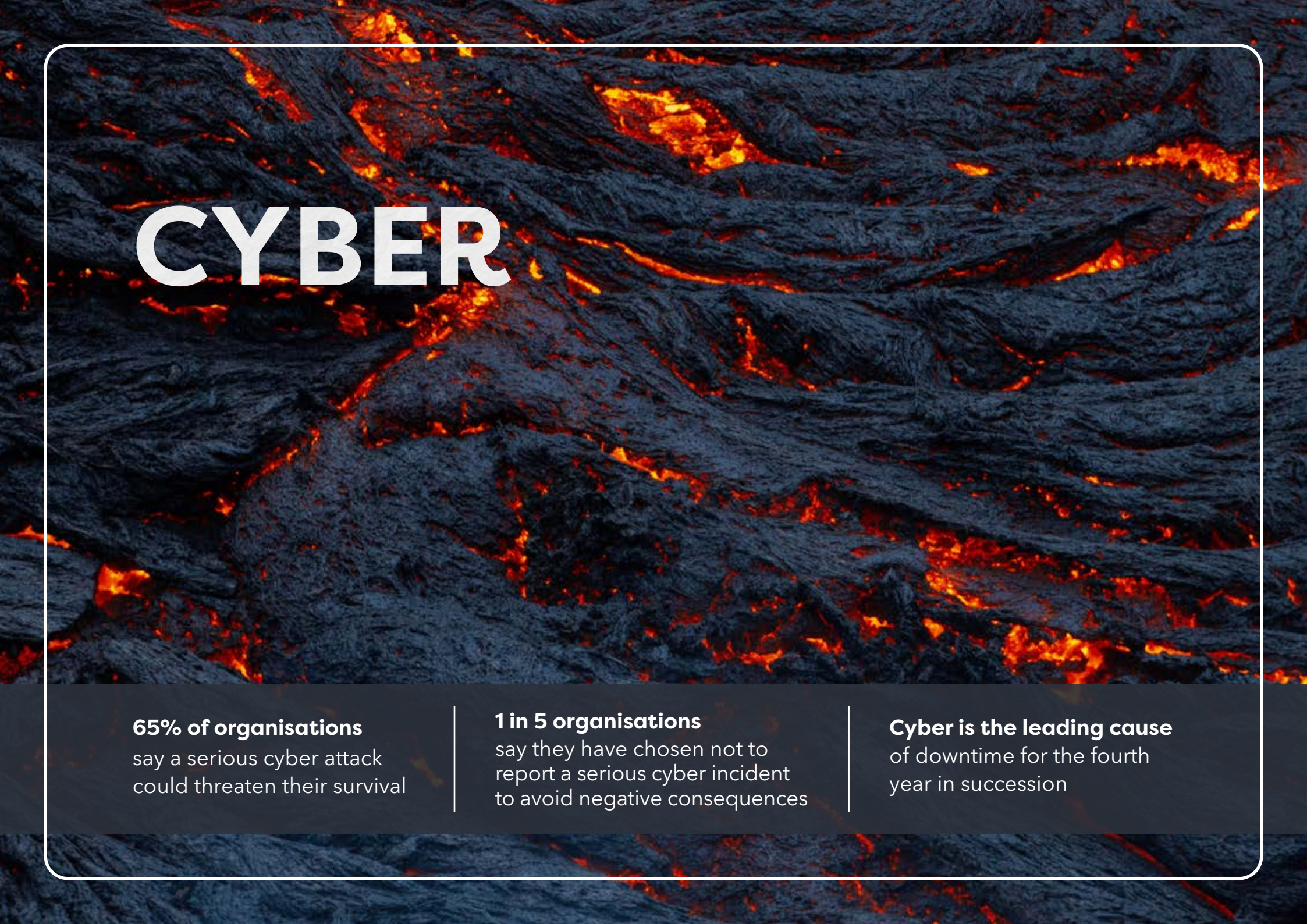
Supplier resilience is another growing concern. **1 in 4 organisations experienced a cyber incident originating from a supplier or third party**. Alarmingly, nearly half of organisations (48%) continue working with suppliers despite known resilience or security concerns.

There is progress. **90% of organisations now have business continuity plans**, and 4 in 5 of those are up to date. Adoption of air-gapped and immutable backups also continues to grow, putting more organisations in a stronger position to recover from cyber attacks. That recovery capability is reflected in ransomware response: even as attacks rise, organisations continue to hold the line on payments. **1 in 4 experienced a ransomware attack in the last 12 months.** Of those, **only 18% paid the ransom,** while **59% recovered from backups instead**.

Confidence in continuity and recovery capability is also growing, with **76% of organisations believing they are more resilient than they were 12 months ago**. That confidence is not always backed by testing, however, and likely exceeds capability in many cases.

The overall picture is one of progress and pressure. Organisations are strengthening their resilience posture, but the threats they are facing are becoming harder to manage through isolated teams, plans or controls. This helps explain why **"integrating IT and business resilience" is the most-cited priority for resilience in 2026.**

Modern incidents cut across cyber security, IT operations, business continuity, crisis communications, suppliers and executive decision-making. Resilience now has to operate across those boundaries.



65% of organisations
say a serious cyber attack could threaten their survival

1 in 5 organisations
say they have chosen not to report a serious cyber incident to avoid negative consequences

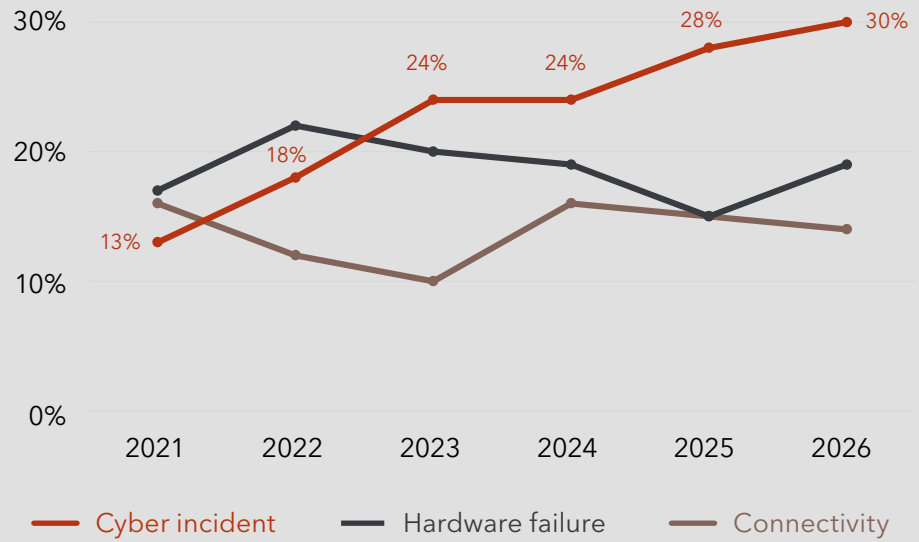
Cyber is the leading cause
of downtime for the fourth year in succession

Cyber the #1 cause of downtime and data loss

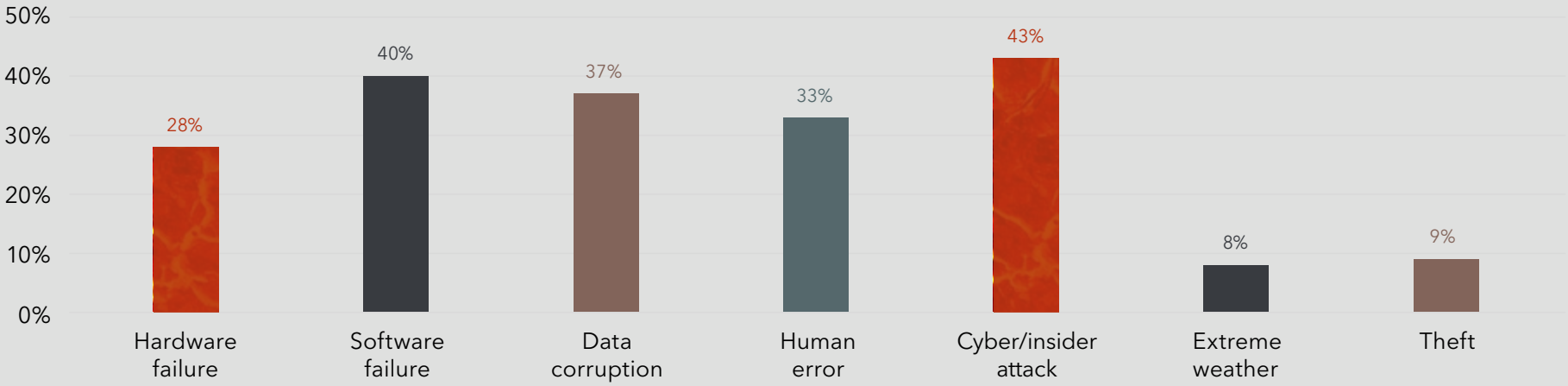
Cyber is the leading cause of downtime for the fourth year in succession and continues to drive data loss.

5 years ago, only 13% of organisations cited cyber as their biggest cause of downtime. That figure has now more than doubled to 30%.

Biggest causes of IT downtime



What were the causes of any data loss over the last 12 months?

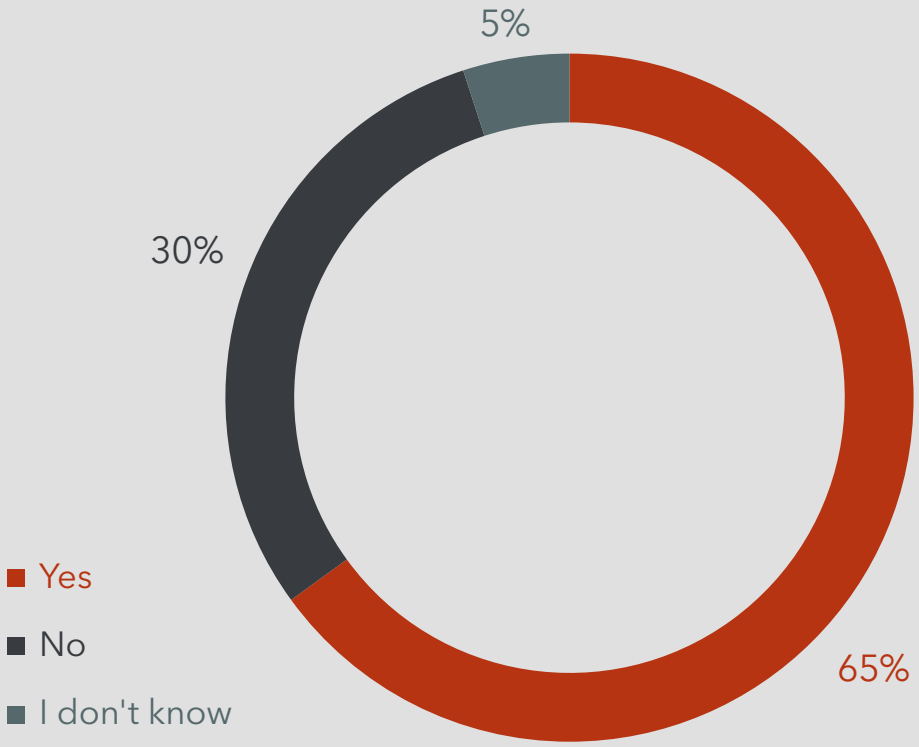


Existential threat posed by cyber

65% of organisations say a serious cyber attack could threaten their survival.

Once viewed primarily as an IT issue, cyber is now recognised as a critical threat to operational resilience.

Do you believe a serious cyber attack could threaten your organisation's survival?

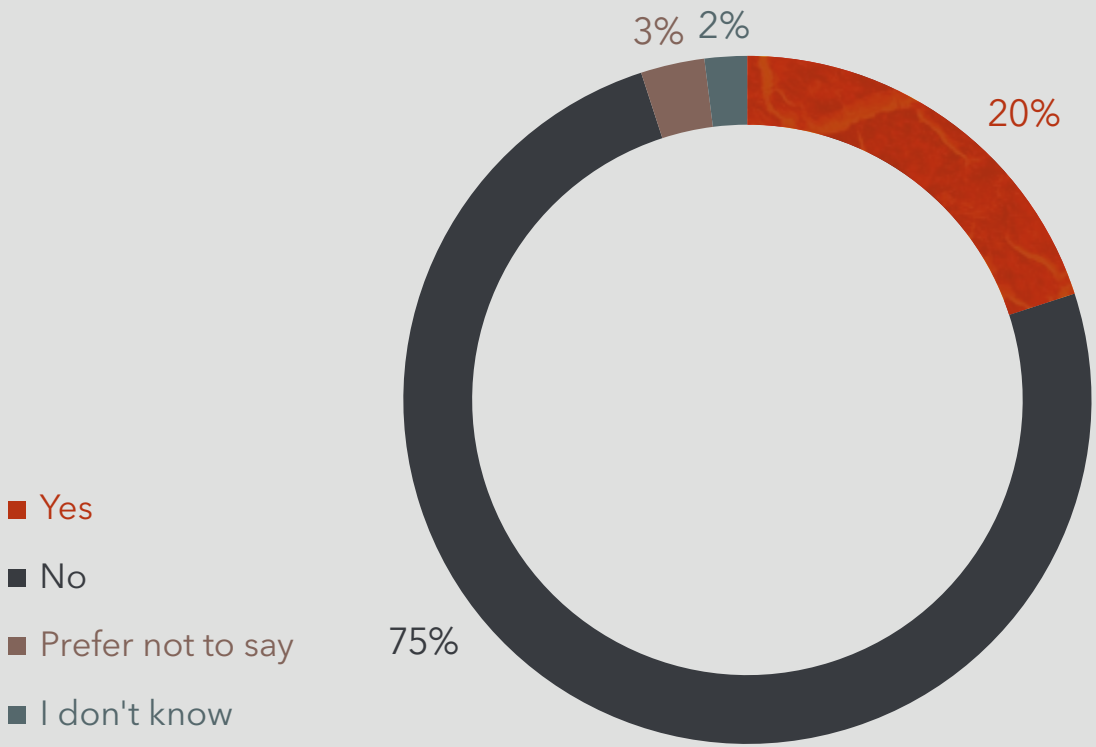


Cyber incidents kept behind closed doors

The full scale of serious cyber incidents may be hidden from public view.

1 in 5 organisations say they have chosen not to report a serious cyber incident to avoid negative consequences.

Has your organisation ever chosen not to report a serious cyber incident to avoid negative consequences?



Organisations planning for the worst

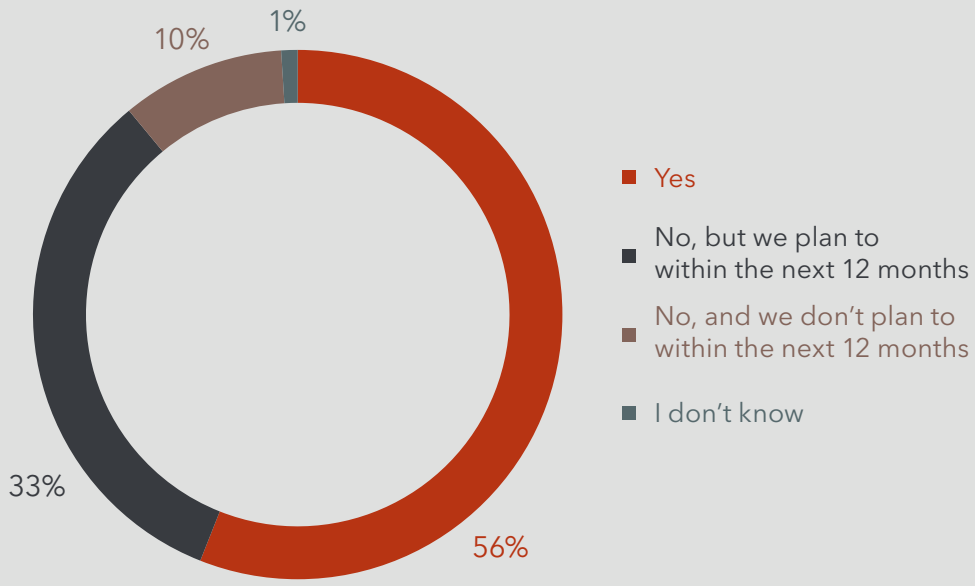
Organisations are preparing for worst-case scenarios through “minimum viable company” planning and “scorched earth” scenario testing.

57% say they have a formal minimum viable company strategy in place.

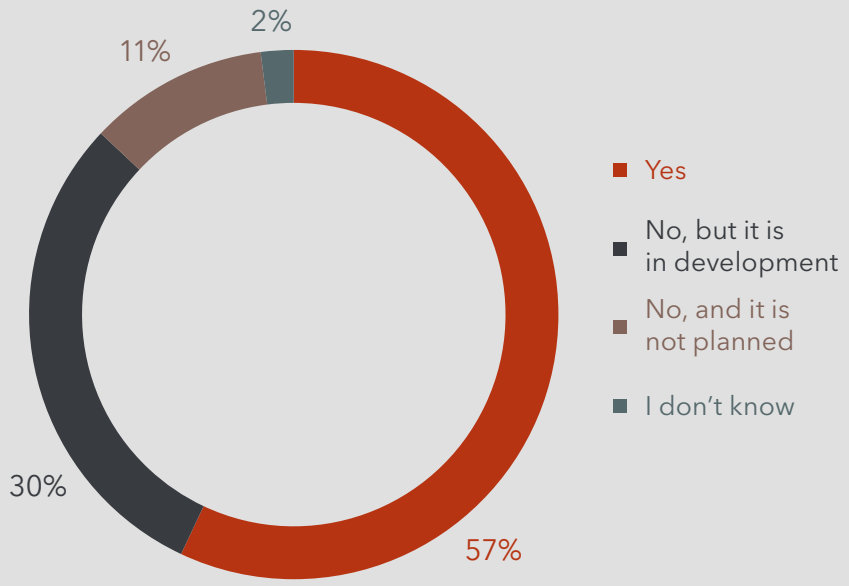
56% say they have tested their ability to operate following total IT loss in a “scorched earth” scenario.

As these are still emerging concepts in resilience, organisations are likely defining and applying them in different ways. The findings are therefore best viewed as evidence of a growing focus on extreme disruption planning, rather than consistent implementation.

Have you tested your ability to operate following a total loss of all IT systems?



Do you have a formal minimum viable company strategy in place?



RANSOMWARE

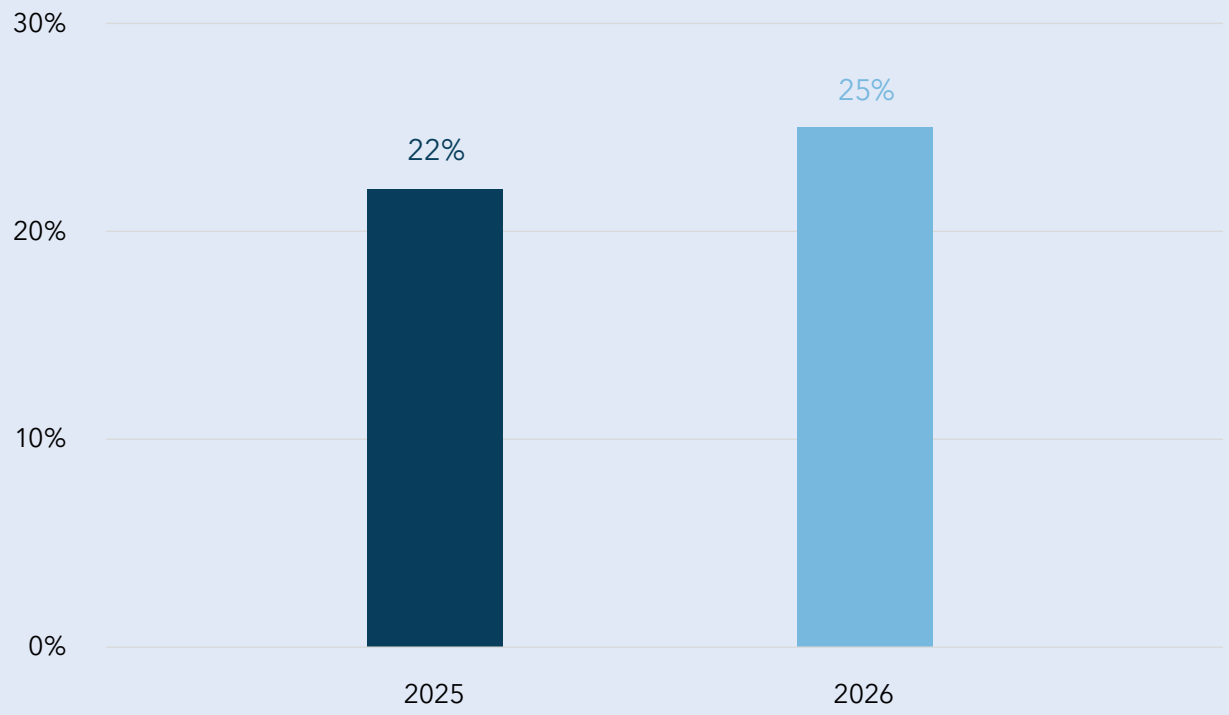
1 in 4 organisations
experienced a ransomware attack in the last 12 months

Only 18% paid the ransom
while 59% recovered from backups instead

Ransomware attacks rising

1 in 4 organisations experienced a ransomware attack in the last 12 months, up from 22% in 2025.

Organisations that suffered a ransomware attack in the last 12 months

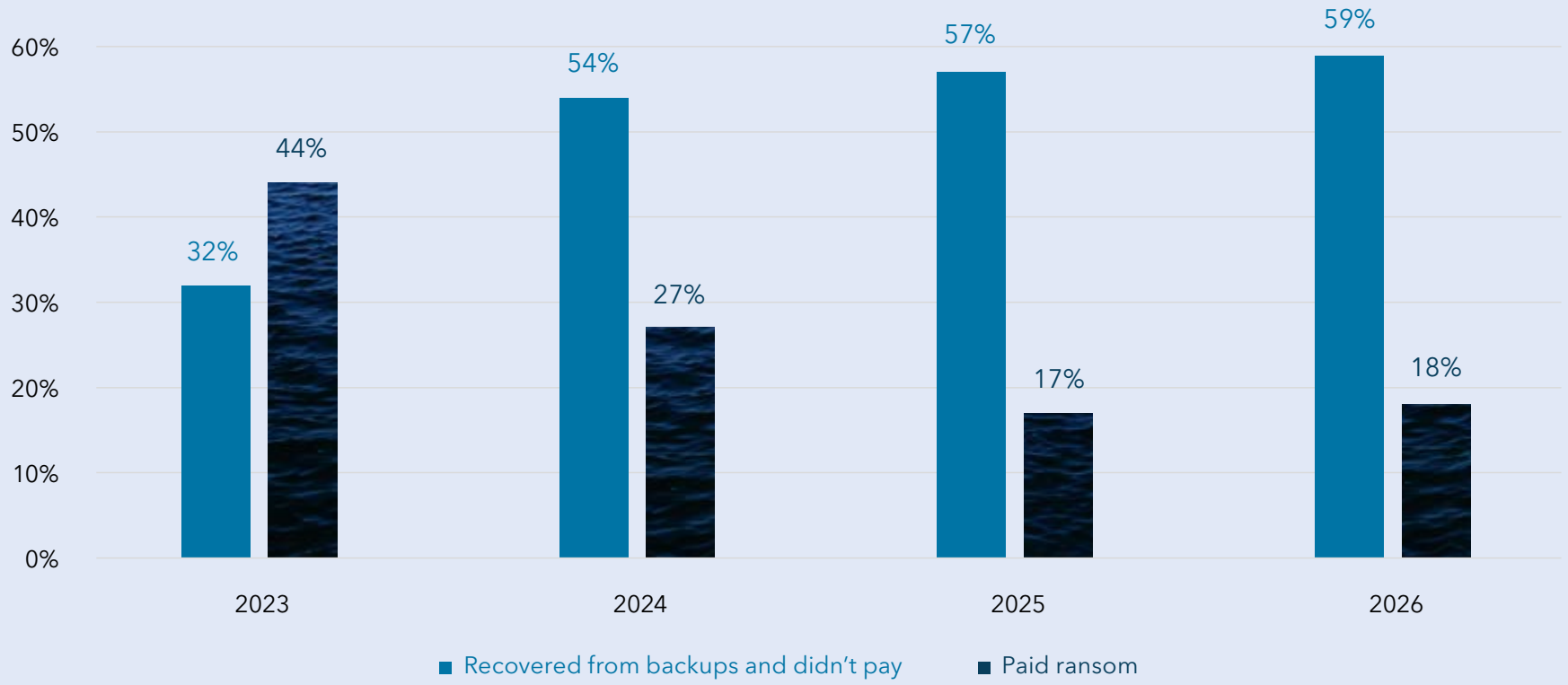


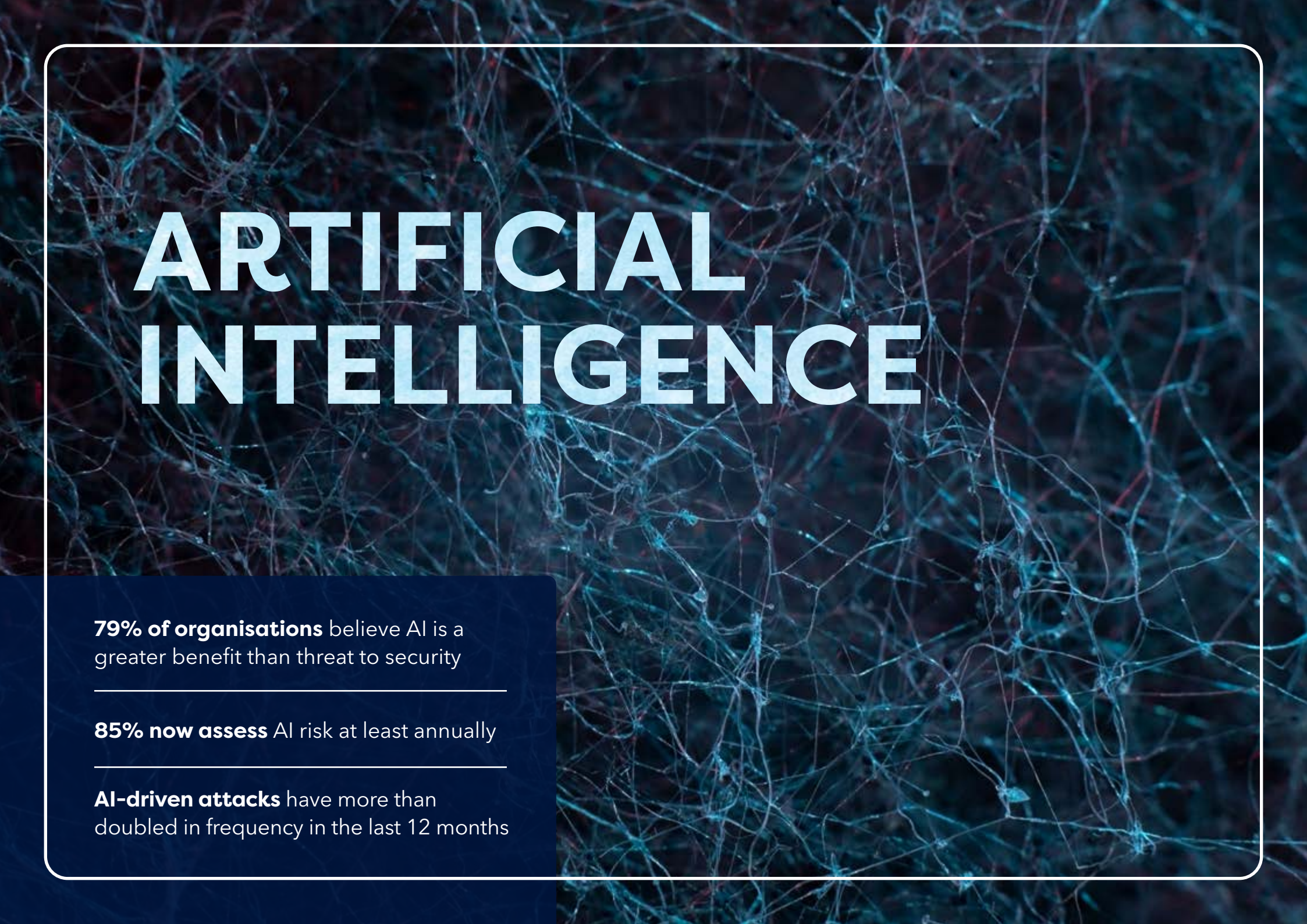
Hard line held on ransomware payments

Only 18% of organisations hit by a ransomware attack paid the ransom.

The number of organisations refusing to pay and recovering from backups instead has reached 59%, continuing an encouraging 4-year growth trend.

How did you respond to the ransomware attack?





ARTIFICIAL INTELLIGENCE

79% of organisations believe AI is a greater benefit than threat to security

---

85% now assess AI risk at least annually

AI-driven attacks have more than doubled in frequency in the last 12 months

Growing optimism around AI

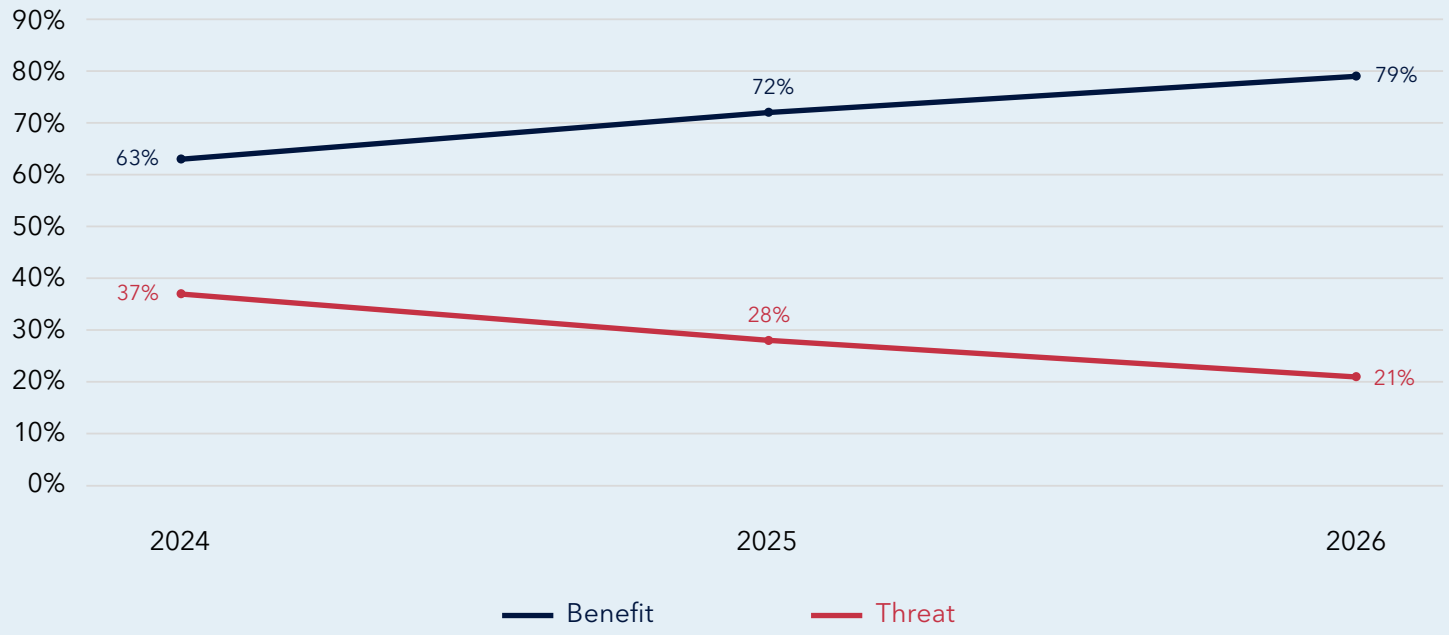
The number of organisations that see AI as a greater benefit than threat continues to grow, reaching 79% in 2026.

Smaller organisations remain more cautious: 59% see AI as a net benefit, unchanged from 2025.

79%

see AI as a security benefit

Is AI a greater threat or benefit to security in your organisation?

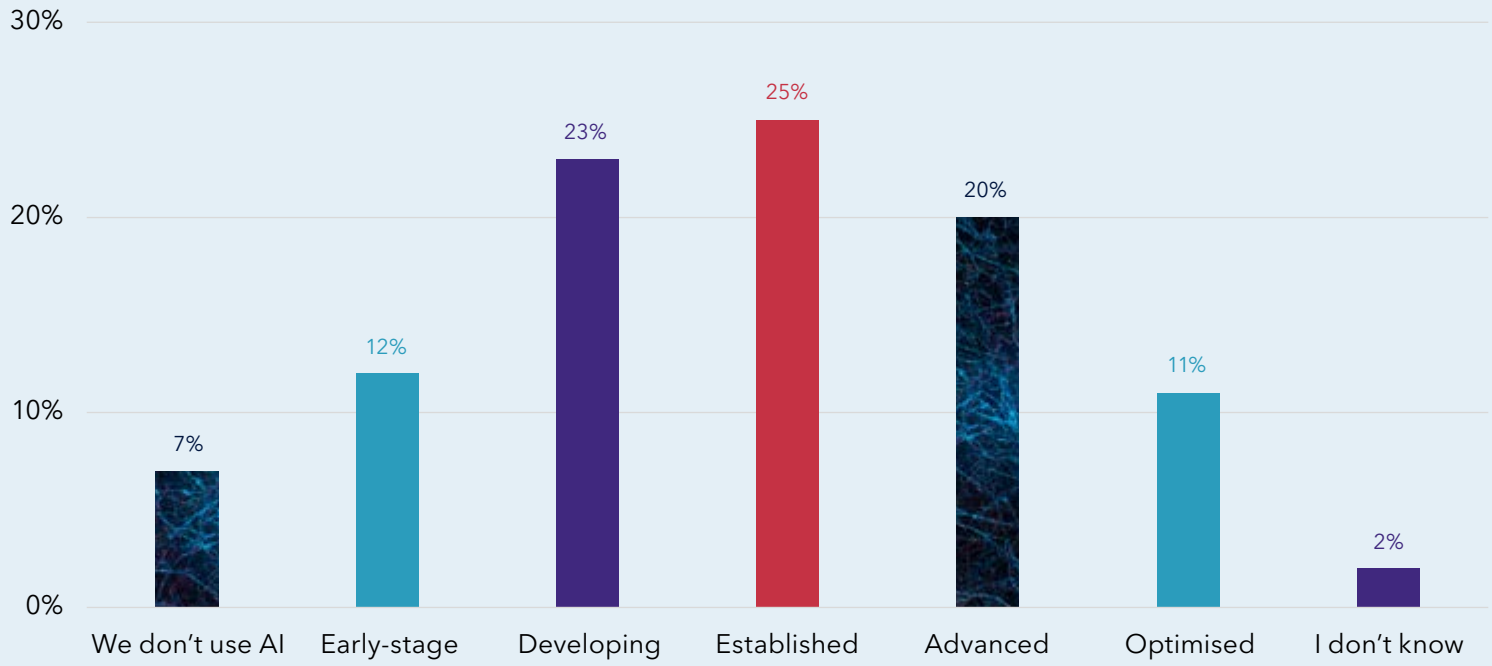


Resilience teams embracing AI

The vast majority of resilience teams (93%) now use AI in some form.

Around a third of organisations (31%) rate the maturity of their AI programme as advanced or optimised.

How would you describe the maturity of AI use in your risk and resilience team?



AI remains a double-edged sword

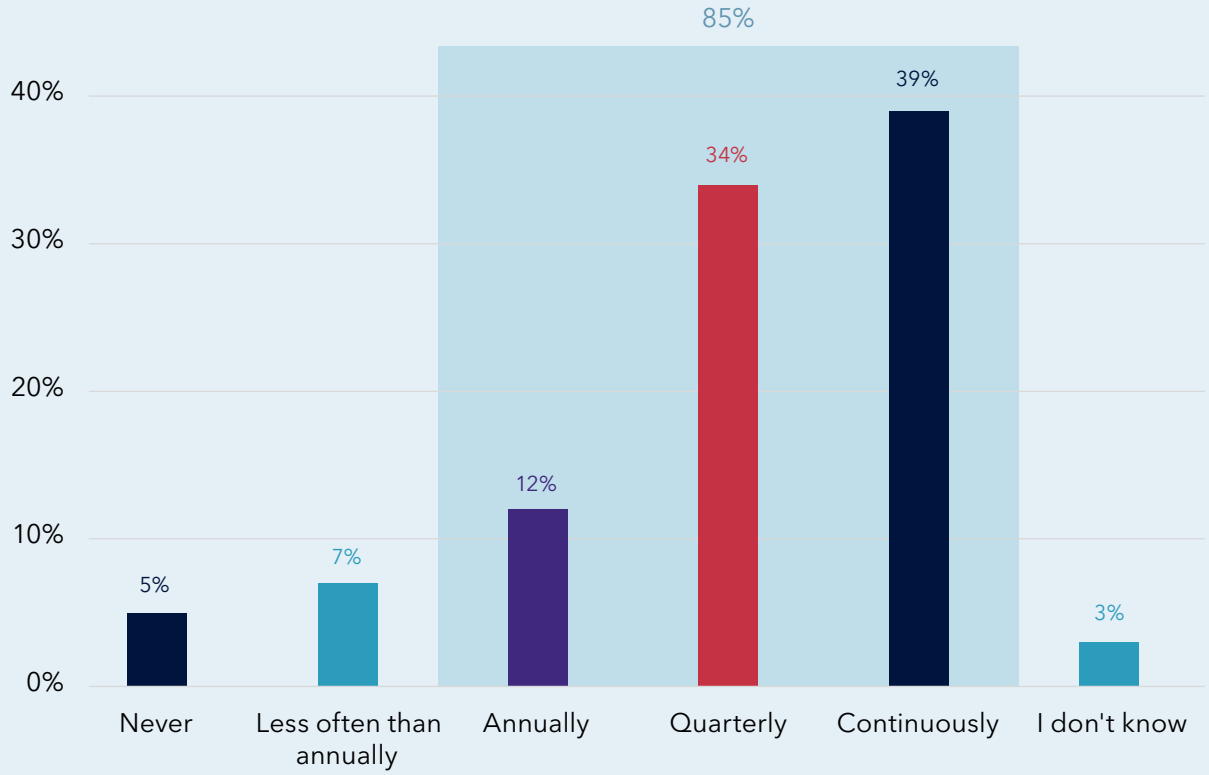
Organisations are responding fast to both the opportunities and risks presented by AI.

85% now assess AI risk at least annually.

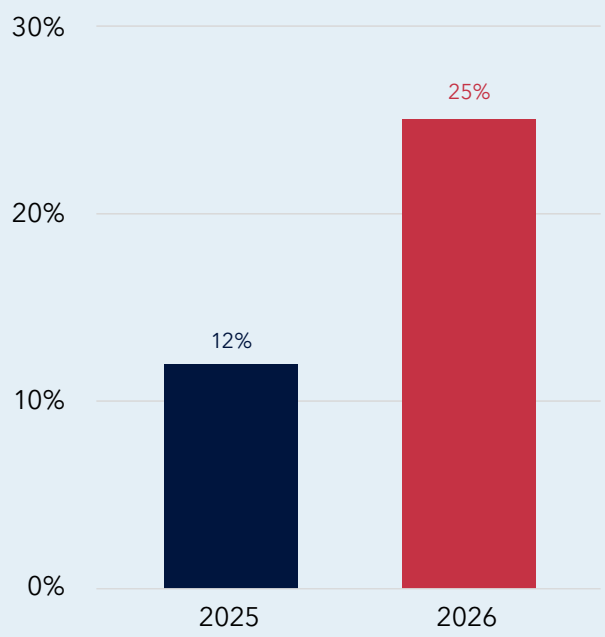
For the second year running, AI-driven cyber threats were identified as the biggest resilience challenge facing organisations over the next 5 years.

With AI-driven attacks more than doubling in frequency this year, the challenge is already materialising.

How regularly do you review AI risk?



Organisations affected by AI-driven cyber attacks



SUPPLY CHAIN

48% continue working with risky suppliers

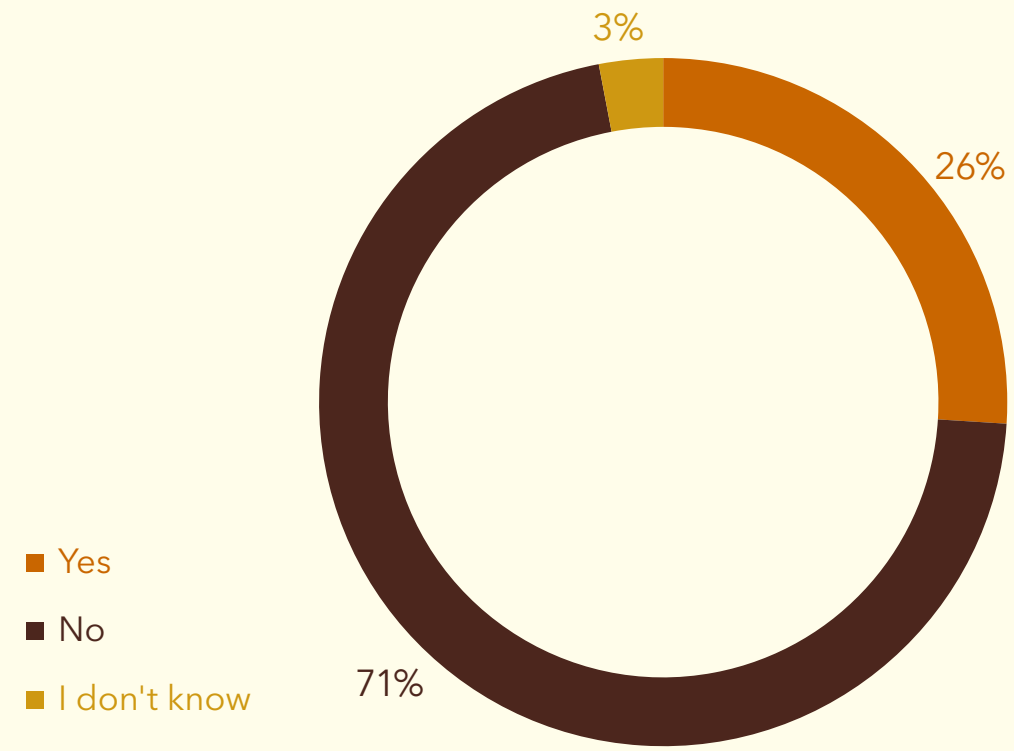
1 in 4 organisations experienced a cyber incident originating from a supplier or third party in the last 12 months

26% identify dependence on suppliers as a main barrier to improving resilience

Supply chain leaving organisations exposed

1 in 4 organisations experienced a cyber incident originating from a supplier or third party, with large organisations disproportionately affected.

In the last 12 months, has your organisation experienced a cyber incident originating from a supplier or third party?

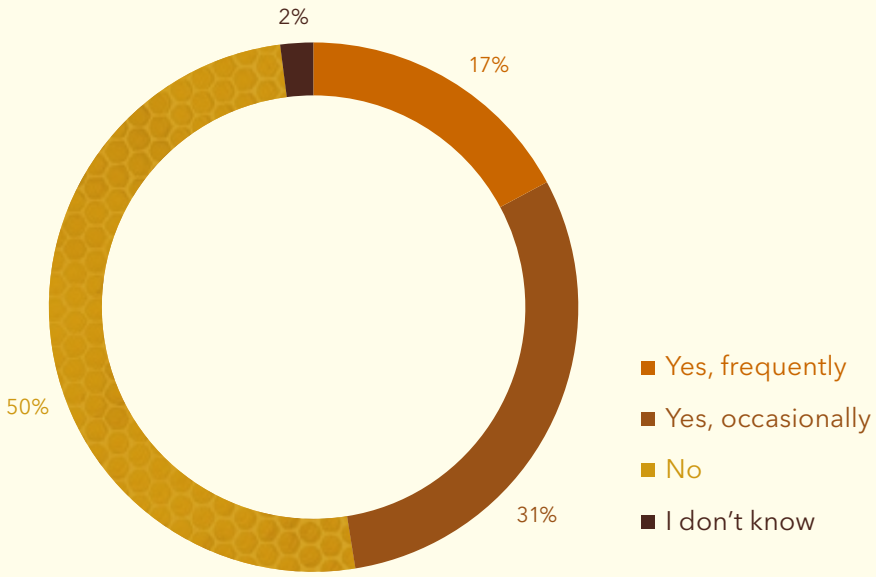


Known supplier risks being tolerated

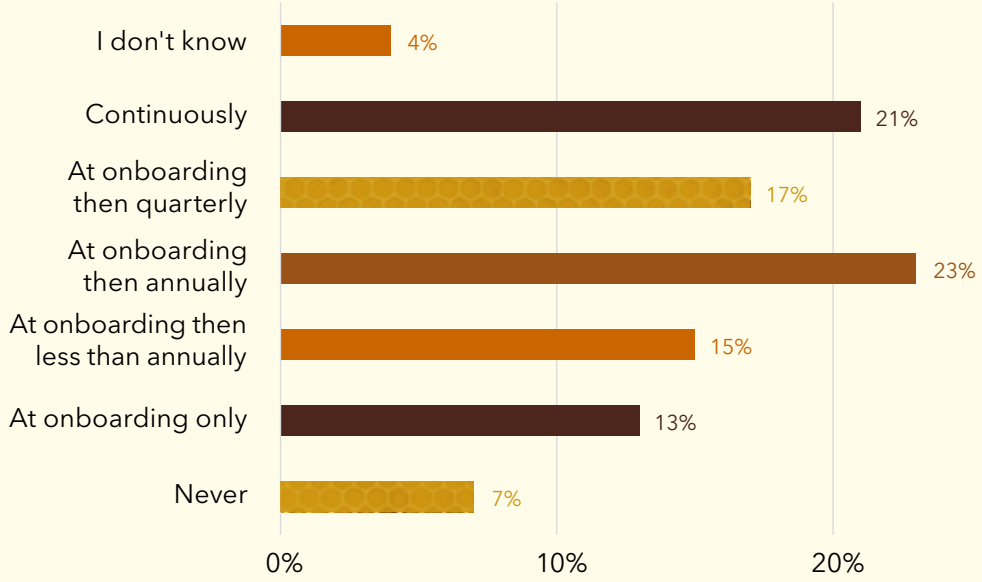
Nearly half of organisations (48%) continue working with suppliers despite known resilience or security concerns.

Organisations are aware of the risk, with 9 in 10 assessing supplier resilience at least at onboarding, but they may lack viable alternatives. 1 in 4 identify dependence on suppliers as a main barrier to improving resilience.

Has your organisation continued working with a supplier despite known security or resilience concerns?



When does your organisation assess supplier resilience?



CONTINUITY & RESILIENCE

9 in 10 organisations have business continuity plans in place

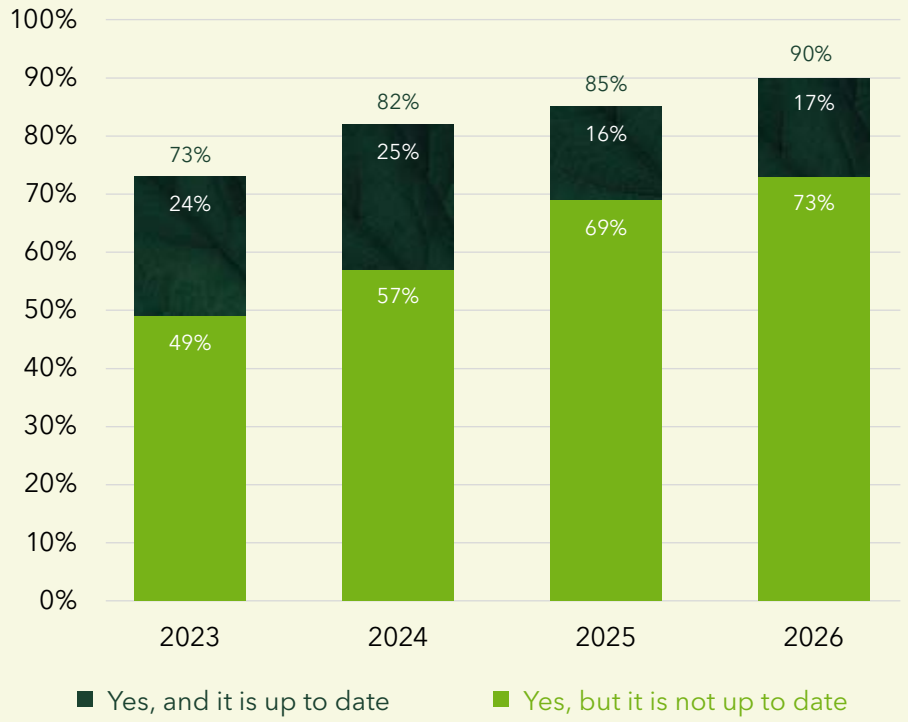
51% believe their organisation treats resilience as a box-ticking exercise

43% say resilience only becomes a focus after something goes wrong

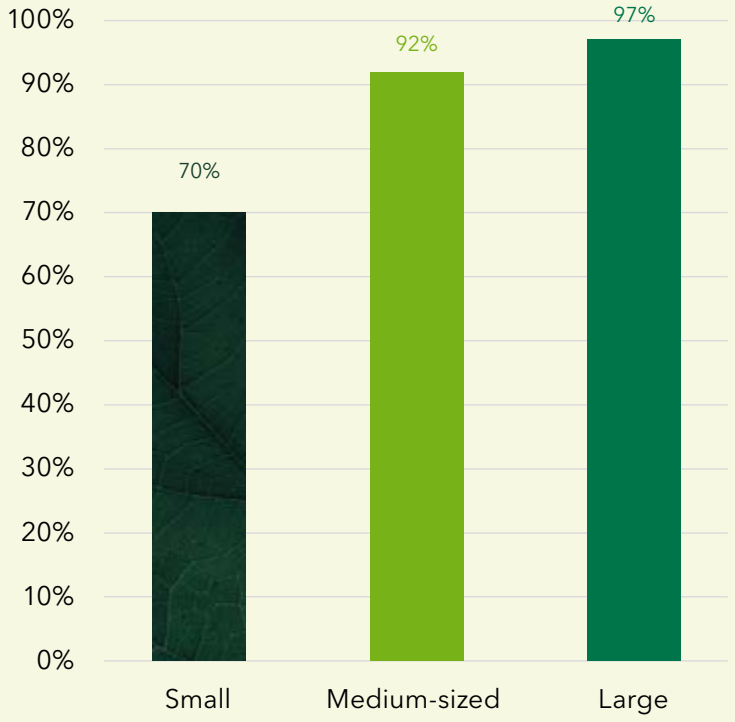
More organisations than ever have a business continuity plan

Business continuity planning has reached a new high. In 2026, **90% of organisations have a business continuity plan,** and 81% of those are up to date.

Do you have a business continuity plan?



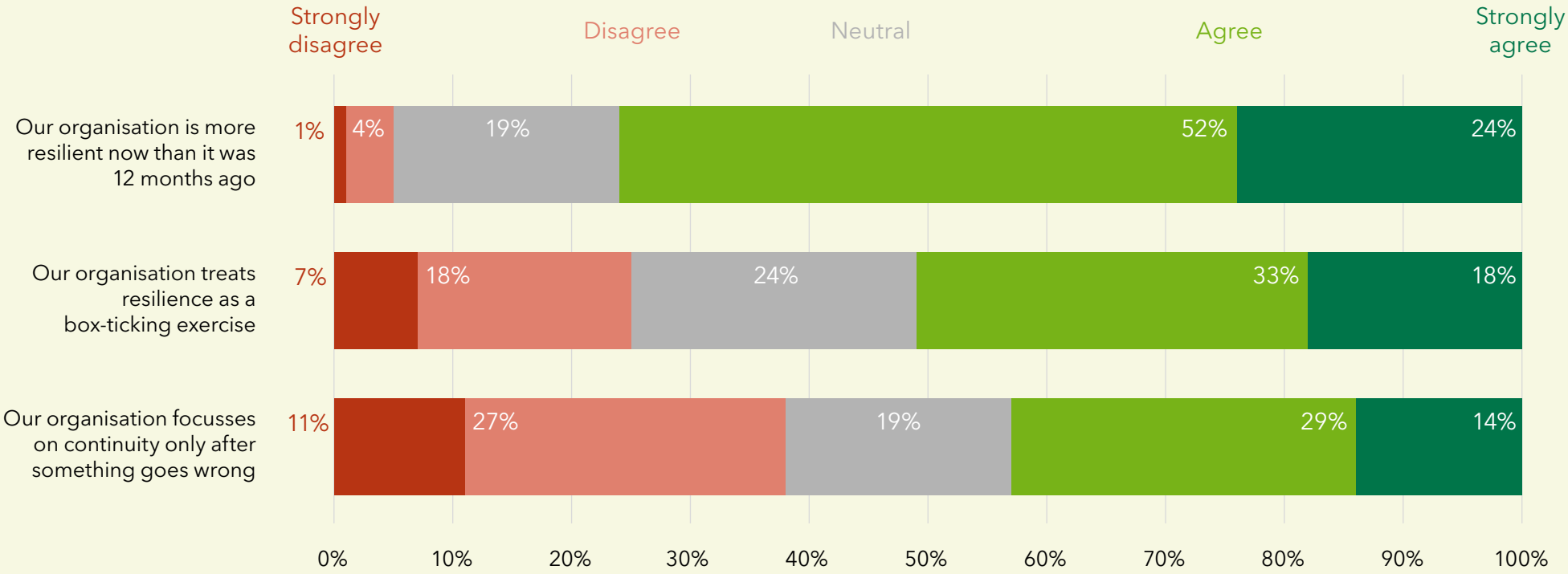
Organisations with a business continuity plan



Resilience improving but still reactive

While 3 in 4 organisations believe they are more resilient than they were 12 months ago, many still appear to approach resilience reactively:

51% believe their organisation treats resilience as a box-ticking exercise, and 43% say resilience only becomes a focus after something goes wrong.

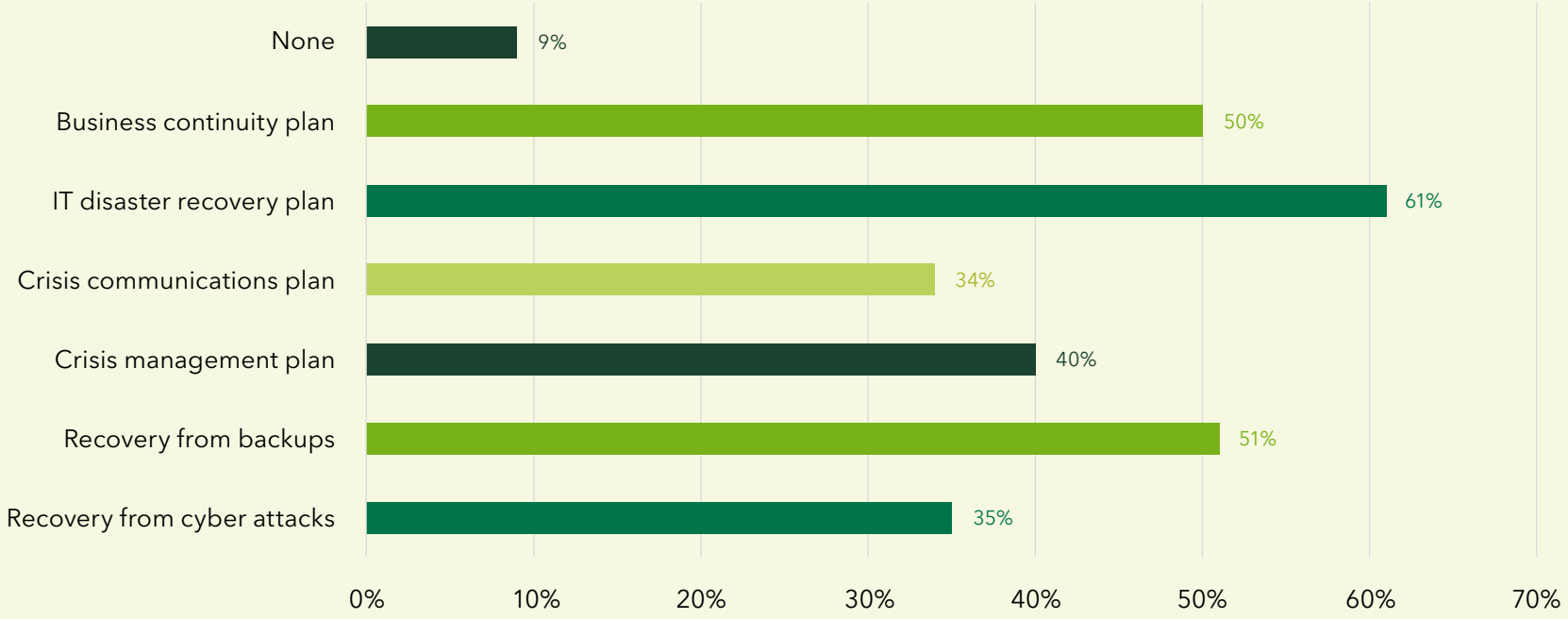


Foundations to build on in testing and exercising

Only 9% of organisations have not tested any plans or recovery processes in the last 12 months. However, the breadth of testing is a concern.

Only 35% have tested or exercised their recovery from cyber attacks, even as high-profile attacks on some of the UK's best-known brands put the severe consequences of a breach in focus.

Which of the following have you tested or exercised in the last 12 months?

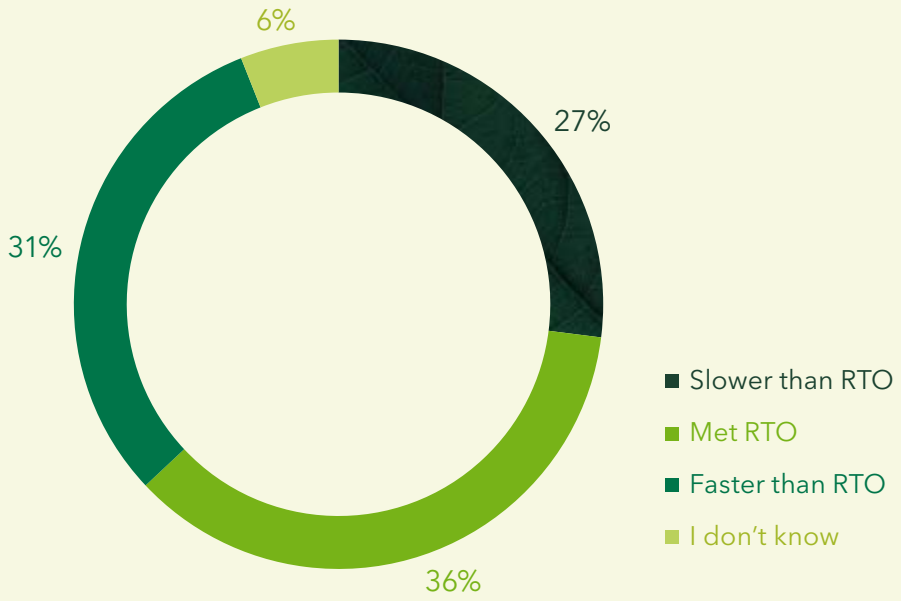


Recovery targets still being missed

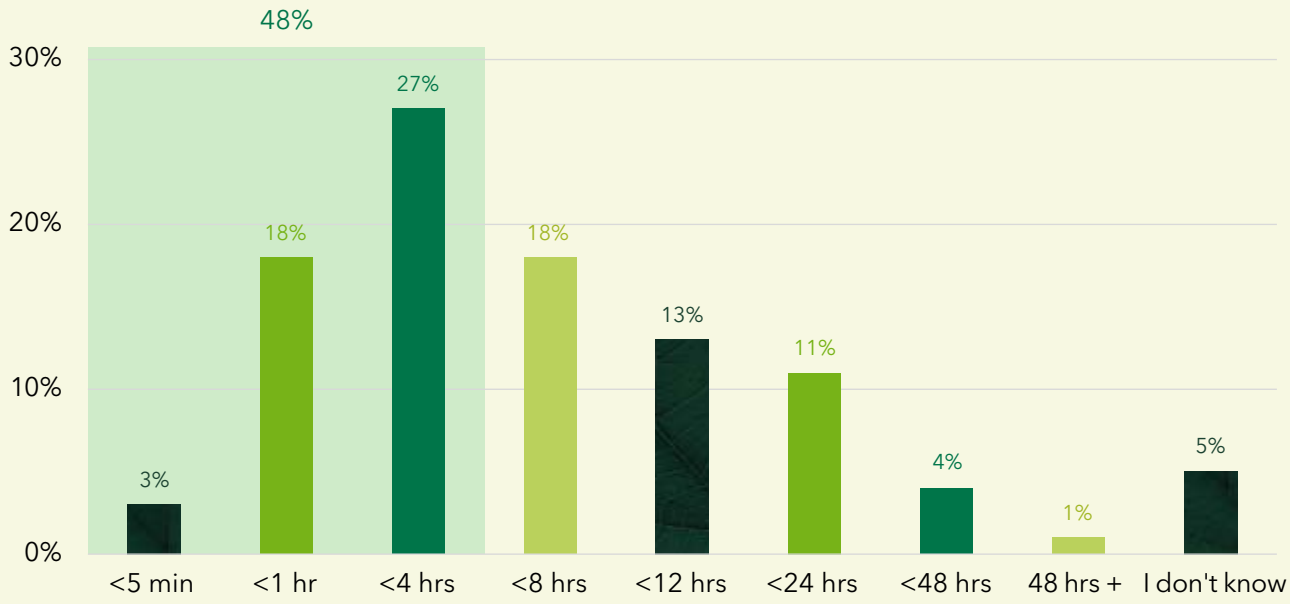
In 2026, nearly half of organisations (48%) have a recovery time objective (RTO) of less than 4 hours.

While most organisations met or exceeded their RTO in their most recent test or incident, 27% fell short.

Recovery time objective vs actual recovery time



What is your recovery time objective?



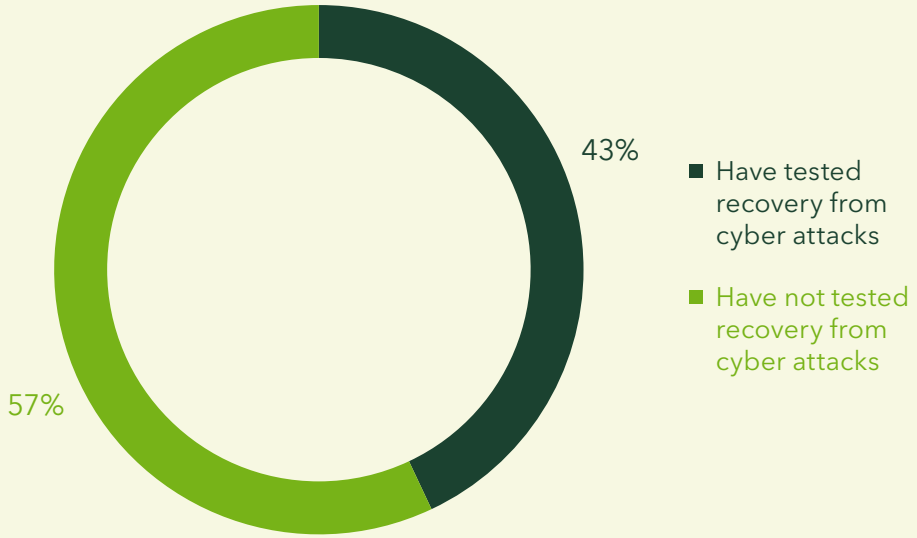
Confidence exceeding capability

Confidence in recovery and resilience is rising, and 3 in 4 organisations believe they are more resilient now than they were 12 months ago.

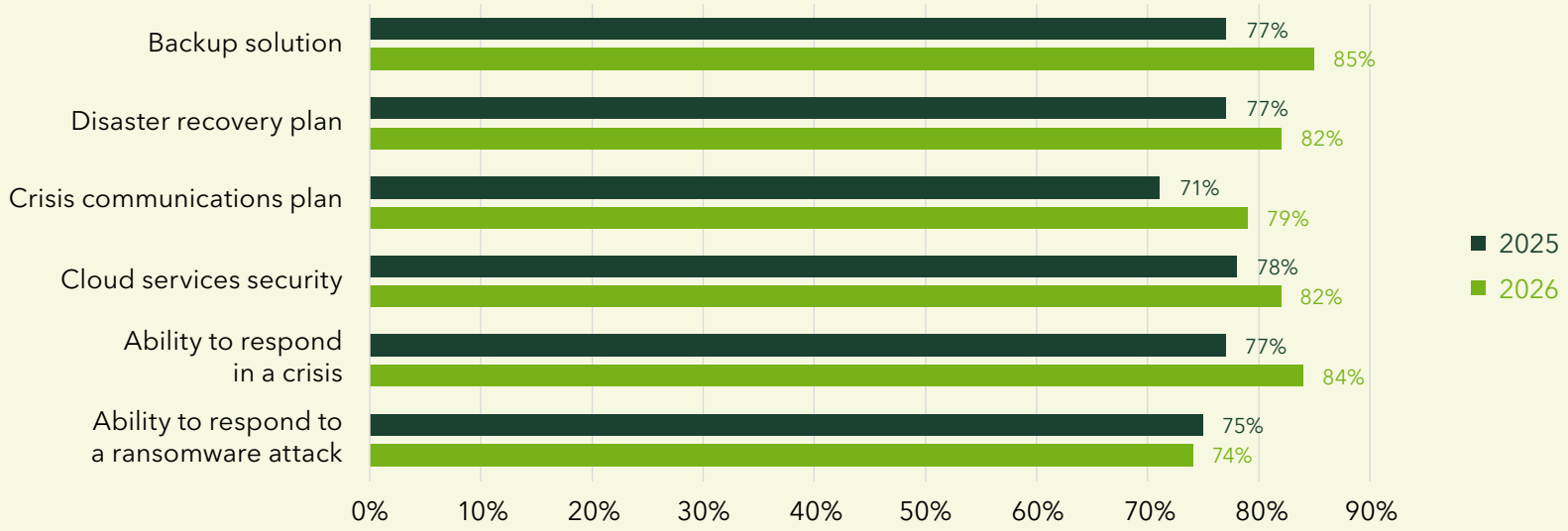
However, that confidence likely exceeds capability, with many organisations expressing high levels of confidence despite never fully testing their recovery capabilities:

Only 43% of organisations that describe themselves as “very confident” in their ability to respond to a ransomware attack have tested recovery from cyber attacks in the last 12 months.

Organisations that are “very confident” in their ability to respond to a ransomware attack.



We are confident in our…



THE STATE OF IT RESILIENCE

Top priority for resilience:
Integrating IT and business resilience

Top barrier to resilience:
Complexity of IT environment

Top challenge over the next 5 years:
AI-driven cyber threats

IT resilience priorities for 2026

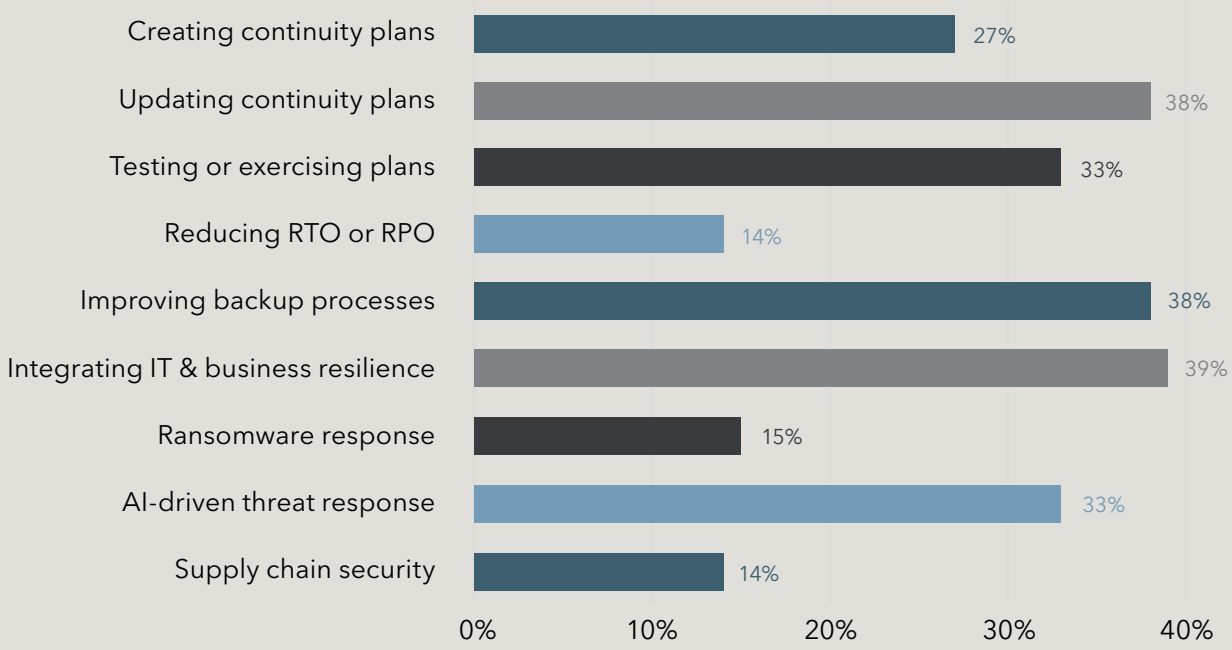
Integrating IT and business resilience is the top resilience priority for organisations in 2026, followed by **updating continuity plans** and **improving backup processes**.

Large organisations in particular are committed to integrating resilience operations, with nearly half (48%) identifying it as a priority this year.

Top 3 resilience priorities

1. Integrating IT and business resilience
2. Updating continuity plans
3. Improving backup processes

What are your priorities for IT resilience this year?



Barriers to resilience

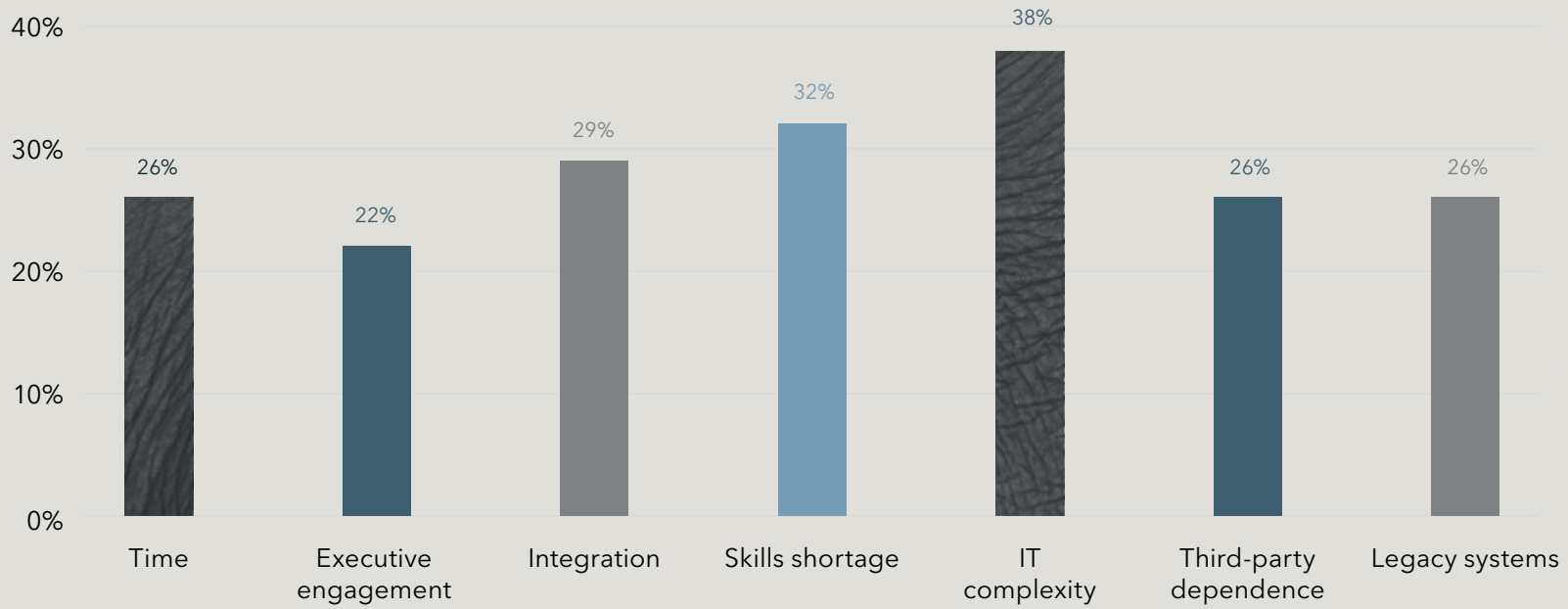
Complex IT environments are the biggest barrier to improving resilience in 2026.

Skills shortage, lack of time, lack of integration across resilience operations, supplier dependence and legacy systems are also holding many organisations back.

Top 3 barriers to resilience

1. IT complexity
2. Skills shortage
3. Integration across resilience operations

What are your barriers to improving resilience?



5-year resilience horizon

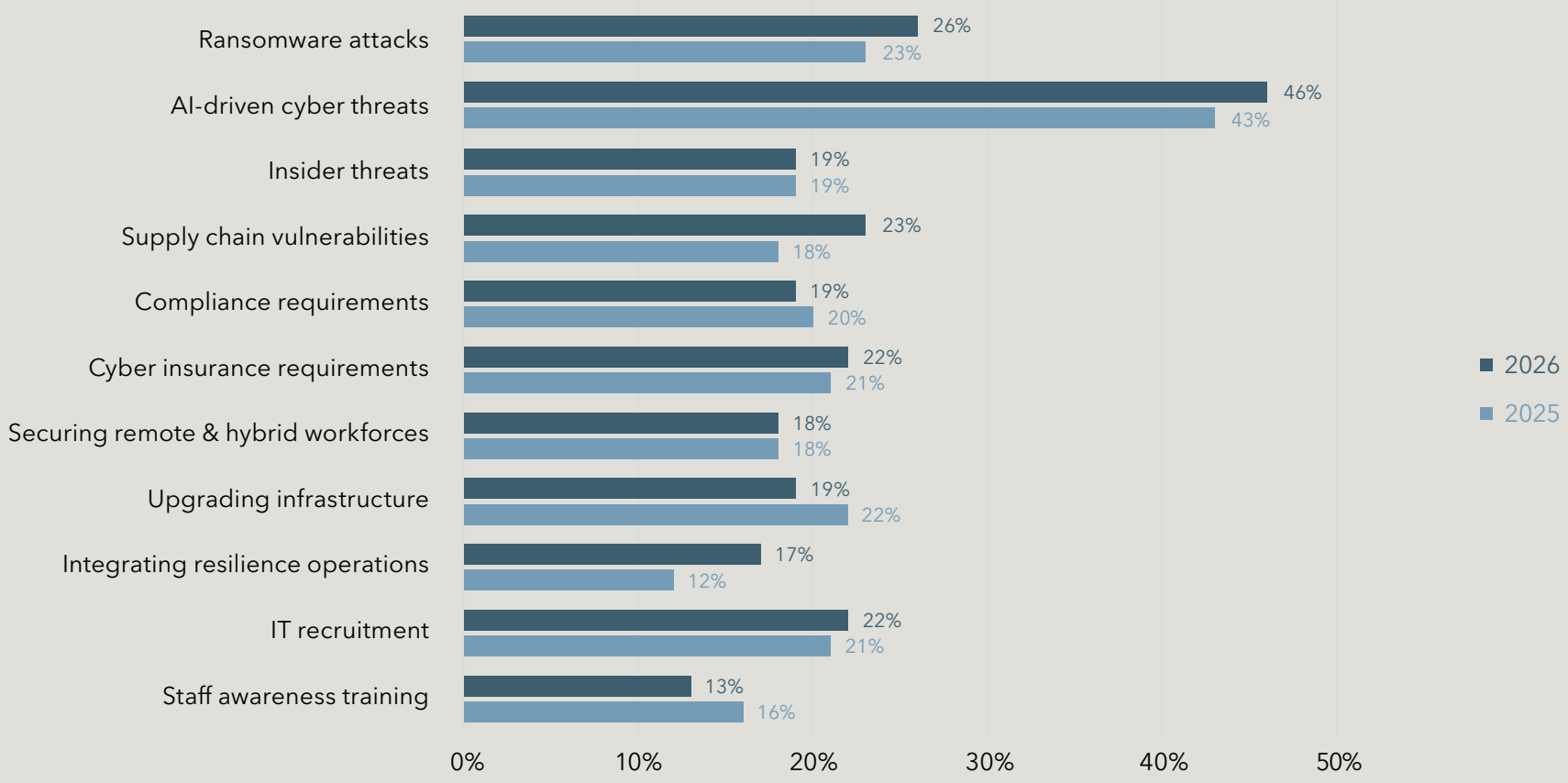
AI-driven cyber threats remain the biggest resilience challenge organisations expect to face over the next 5 years.

Concerns around **supply chain vulnerabilities** and **integrating resilience operations** are growing fastest, rising by around 30% and 40% respectively since 2025.

Top challenges over the next 5 years

1. AI-driven cyber threats
2. Ransomware attacks
3. Supply chain vulnerabilities

What will be your biggest IT resilience challenges over the next 5 years?



APPENDIX

Complete responses

Q1. What best describes your business sector?

Banking and finance	9.20%
Charity and NGO	0.20%
Construction and property	5.40%
Consumer goods	0.60%
Education	2.60%
Engineering	3.80%
Health	3.60%
Industrial	0.20%
Legal	0.60%
Leisure	0.60%
Manufacturing	7.80%
Media and marketing	1.40%
Natural resources	0.60%
Pharmaceuticals	0.80%
Professional services	6.00%
Public sector	1.80%
Retail	8.60%
Technology	40.40%
Telecommunications	2.00%
Transport	2.40%
Utilities	0.60%
Other	0.80%

Q2. What is your position within the business?

Corporate/Board-level responsible for IT	21.60%
Director-level responsible for IT	33.40%
IT Manager	33.80%
IT Technical Specialist	6.40%
IT Consultant	4.80%

Q3. How many employees does your company have?

< 25	10.80%
25–49	6.80%
50–99	6.80%
100–249	16.80%
250–499	18.00%
500–999	16.80%
1000–4999	17.80%
5000+	6.20%

Q4. How many employees are in your IT department?

< 5	12.80%
5–10	13.80%
11–15	16.00%
16–30	23.00%
31–100	22.80%
> 100	11.60%

Q5. Where is your UK head office located?

North East	4.40%
North West	13.80%
Yorkshire and the Humber	7.00%
East Midlands	5.80%
West Midlands	9.00%
East of England	5.00%
London	30.20%
South East	9.40%
South West	4.80%
Scotland	6.00%
Wales	3.80%
Northern Ireland	0.80%

Q6. What is your annual turnover?

< £5m	15.60%
£5 - 9.9m	8.60%
£10 - 24.9m	8.80%
£25 – 49.9m	10.80%
£50 – 99.9m	12.20%
£100 – 249.9m	11.60%
£250 – 499.9m	9.60%
£500 – 999.9m	15.00%
> £1bn	7.80%

Q7. Do you have a business continuity plan?

Yes, and it is up to date	72.80%
Yes, but it is not up to date	17.20%
No, but we will within the next 12 months	4.20%
No, and we don't intend to implement one within the next 12 months	4.40%
I don't know	1.40%

Q8. Alongside your business continuity plan, do you have any of the following plans?

IT Disaster recovery plan

Yes, and it is up to date	73.78%
Yes, but it is not up to date	16.44%
No, but we will within the next 12 months	6.67%
No, and we don't intend to implement one within the next 12 months	2.00%
I don't know	1.11%

Crisis communications plan

Yes, and it is up to date	60.89%
Yes, but it is not up to date	21.78%
No, but we will within the next 12 months	10.22%
No, and we don't intend to implement one within the next 12 months	5.11%
I don't know	2.00%

Crisis management plan

Yes, and it is up to date	68.89%
Yes, but it is not up to date	17.11%
No, but we will within the next 12 months	8.44%
No, and we don't intend to implement one within the next 12 months	4.44%
I don't know	1.11%

Q9. Which of the following have you tested or exercised in the last 12 months? Select all that apply.

None of the above	8.80%
Business continuity plan	50.00%
IT Disaster recovery plan	61.00%
Crisis communications plan	34.00%
Crisis management plan	40.40%
Recovery from backups	50.80%
Recovery specifically from cyber attacks	34.60%
I don't know	1.20%

Q10. Have you tested your ability to operate following a total loss of all IT systems (a "scorched earth" scenario)?

Yes	56.00%
No, but we plan to within the next 12 months	32.80%
No, and we don't plan to within the next 12 months	9.80%
I don't know	1.40%

Q11. What were the causes of any data loss over the last 12 months? Select all that apply.

Hardware failure	28.20%
Software failure	39.60%
Data corruption	37.40%
Human error	33.20%
Internal security breach (member of staff)	18.20%
Cyber attack	32.60%
Extreme weather or flooding	7.80%
Theft	8.60%
I don't know	0.60%
None	16.60%
Other	0.40%

Q12. What was the biggest cause of IT downtime for your organisation in the last 12 months?

Extreme weather or flooding	3.20%
Hardware failure	18.60%
Cyber incident	29.80%
Upgrades/patches	12.00%
Cloud outages	11.40%
Connectivity issues	14.00%
I don't know	0.00%
We didn't experience any downtime in the last 12 months	11.00%
Other	0.00%

Q13. What are your priorities for IT resilience this year? Select up to three.

Creating continuity plans	26.60%
Updating continuity plans	38.20%
Testing or exercising plans	33.20%
Reducing RTO or RPO	14.00%
Improving backup processes	37.60%
Integrating IT and business resilience	38.60%
Ransomware response	15.40%
AI-driven threat response	32.80%
Supply chain security	14.00%
I don't know	2.40%
Other	0.80%

Q14. What are your main barriers to improving resilience? Select up to three.

Lack of time	25.80%
Lack of executive engagement	21.80%
Lack of integration across resilience operations	29.20%
Skills shortage	32.40%
Complexity of IT environment	38.00%
Dependence on third parties or suppliers	26.40%
Legacy systems	26.00%
I don't know	1.40%
None	13.60%
Other	0.20%

Q15. To what extent do you agree with the following statements?

Our organisation is more resilient now than it was 12 months ago.

Strongly disagree	1.40%
Disagree	4.20%
Neutral	18.40%
Agree	51.80%
Strongly agree	24.20%

Our organisation treats resilience as a box-ticking exercise.

Strongly disagree	7.00%
Disagree	18.00%
Neutral	24.00%
Agree	33.20%
Strongly agree	17.80%

Our organisation focusses on continuity only after something goes wrong.

Strongly disagree	11.00%
Disagree	26.40%
Neutral	19.40%
Agree	29.20%
Strongly agree	14.00%

Q16. What is your current recovery time objective (RTO)?

Less than 5 minutes	3.20%
Less than 1 hour	17.60%
Less than 4 hours	27.40%
Less than 8 hours	18.00%
Less than 12 hours	13.00%
Less than 24 hours	11.60%
Less than 48 hours	3.60%
More than 48 hours	0.80%
I don't know	4.80%

Q17. How did your actual recovery time compare to your recovery time objective (RTO) in your most recent test or incident?

Much slower than RTO	5.20%
Slightly slower than RTO	21.60%
Met RTO	35.40%
Slightly faster than RTO	25.40%
Much faster than RTO	6.20%
I don't know	6.20%

Q18. How long could your organisation survive without its crucial IT systems (what is your maximum tolerable period of disruption)?

Less than 30 minutes	3.20%
Less than 1 hour	6.20%
Less than 4 hours	14.60%
Less than 8 hours	15.20%
Less than 12 hours	11.40%
Less than 1 day	14.40%
Less than 2 days	10.20%
Less than 3 days	7.80%
Less than 1 week	6.40%
Less than 2 weeks	3.60%
Less than 1 month	3.40%
I don't know	3.60%

Q19. Does your organisation have a formal "minimum viable company" strategy to maintain operations during a disruption?

Yes	57.20%
No, but it is in development	29.80%
No, and it is not planned	11.00%
I don't know	2.00%

Q20. How long would it take you to recover your entire IT environment from backups?

Less than 4 hours	17.00%
Less than 8 hours	19.60%
Less than 12 hours	17.00%
Less than 24 hours	20.60%
Less than 48 hours	12.80%
Less than 1 week	6.60%
More than 1 week	2.20%
I don't know	4.20%

Q21. Do you have air-gapped backups?

Yes, logical air-gap	18.20%
Yes, physical air-gap	22.00%
Yes, both logical and physical	35.40%
No	18.20%
I don't know	6.20%

Q22. Do you have immutable backups?

Yes	62.80%
No	28.00%
I don't know	9.20%

Q23. In the last 12 months, has your organisation moved any data or systems from public cloud back to on-premises or private environments (e.g. for resilience, control or security reasons)?

Yes	44.00%
No, but we're planning to in the next 12 months	30.80%
No, and we're not planning to in the next 12 months	23.80%
I don't know	1.40%

Q24. Which of the following cyber threats have you been affected by in the last year? Select all that apply

Phishing	30.60%
Social engineering	21.00%
Ransomware	22.40%
Malware	42.60%
Distributed denial of service	14.40%
Insider breach	15.20%
AI-driven attacks (including deepfakes)	24.60%
None	22.80%
I don't know	0.40%
Other	0.00%

Q25. In the last 12 months, has your organisation experienced a cyber attack that resulted in disruption, data loss or unauthorised access?

Yes	40.00%
No	58.80%
I don't know	1.20%

Q26. How did the cyber attack(s) affect your organisation? Select all that apply.

Revenue loss	27.50%
Data loss	52.00%
Productivity loss	48.50%
Job losses	11.50%
Disciplinary action	29.00%
Reputational damage	16.00%
Regulatory penalties	20.00%
Increased stress	42.50%
Increased workload	38.00%
Decline in staff morale	7.50%
I don't know	0.50%
Other	0.50%

Q27. Do you believe a serious cyber attack could threaten your organisation's survival?

Yes	65.40%
No	29.80%
I don't know	4.80%

Q28. Has your organisation ever chosen not to report a serious cyber incident to avoid negative consequences (e.g. reputational damage)?

Yes	20.00%
No	74.40%
Prefer not to say	3.20%
I don't know	2.40%

Q29. Have you experienced a ransomware attack in the last 12 months?

Yes	25.00%
No	73.20%
I don't know	1.80%

Q30. How did you respond to the ransomware attack?

Recovered from backups and didn't pay	59.20%
Paid ransom	17.60%
Used ransomware decryption tool	22.40%
I don't know	0.80%

Q31. In the last 12 months, has your organisation experienced a cyber incident originating from a supplier or third party?

Yes	25.60%
No	71.20%
I don't know	3.20%

Q32. When does your organisation assess supplier resilience?

Never	6.80%
At onboarding only	12.80%
At onboarding then less often than annually	15.60%
At onboarding then annually	22.80%
At onboarding then quarterly	17.00%
Continuously	21.00%
I don't know	4.00%

Q33. Has your organisation continued working with a supplier despite known security or resilience concerns?

Yes, frequently	16.80%
Yes, occasionally	30.60%
No	50.20%
I don't know	2.40%

Q34. Does your organisation have cyber insurance?

Yes	77.80%
No	17.80%
I don't know	4.40%

Q35. How confident are you in your...

Backup solution

Not applicable	0.60%
Not at all confident	2.00%
I have concerns	12.60%
Fairly confident	47.00%
Very confident	37.80%

Disaster recovery plan

Not applicable	2.20%
Not at all confident	3.00%
I have concerns	12.80%
Fairly confident	46.80%
Very confident	35.20%

Crisis communications plan

Not applicable	2.80%
Not at all confident	3.20%
I have concerns	15.00%
Fairly confident	44.80%
Very confident	34.20%

Cloud services security

Not applicable	3.20%
Not at all confident	1.80%
I have concerns	13.00%
Fairly confident	43.20%
Very confident	38.80%

Ability to respond in a crisis

Not applicable	1.40%
Not at all confident	2.00%
I have concerns	13.40%
Fairly confident	43.80%
Very confident	39.40%

Ability to respond to a ransomware attack

Not applicable	1.80%
Not at all confident	3.80%
I have concerns	20.80%
Fairly confident	41.40%
Very confident	32.20%

Q36. How has your IT budget changed over the last 12 months?

Overall budget

I don't know	1.00%
Decreased	7.40%
Stayed the same	42.20%
Increased	49.40%

Security

I don't know	2.00%
Decreased	4.40%
Stayed the same	38.40%
Increased	55.20%

Backup and DR

I don't know	1.40%
Decreased	4.40%
Stayed the same	58.20%
Increased	36.00%

AI

I don't know	2.80%
Decreased	4.00%
Stayed the same	31.80%
Increased	61.40%

Q37. Is AI a greater threat or benefit to security in your organisation?

Threat	20.60%
Benefit	79.40%

Q38. How regularly do you review AI risk?

Never	5.20%
Less often than annually	6.80%
Annually	11.80%
Quarterly	33.80%
Continuously	39.40%
I don't know	3.00%

Q39. How would you describe the maturity of AI use in your risk and resilience team?

We don't use AI	7.20%
Early-stage (some unstructured use)	11.60%
Developing (defined processes used inconsistently)	22.60%
Established (defined processes used consistently)	25.60%
Advanced (widespread and embedded)	20.20%
Optimised (continuously improved and industry-leading)	10.80%
I don't know	2.00%

Q40. What will be your biggest IT resilience challenges over the next 5 years? Select up to three.

Ransomware attacks	26.00%
AI-driven cyber threats	46.20%
Insider threats	19.40%
Supply chain vulnerabilities	23.40%
Compliance requirements	19.20%
Cyber insurance requirements	22.40%
Securing remote and hybrid workforces	18.40%
Upgrading infrastructure	18.80%
Integrating resilience operations	16.80%
IT recruitment	22.40%
Staff awareness training	12.80%
I don't know	4.80%
Other	0.20%


Databarracks
www.databarracks.com
Databarracks