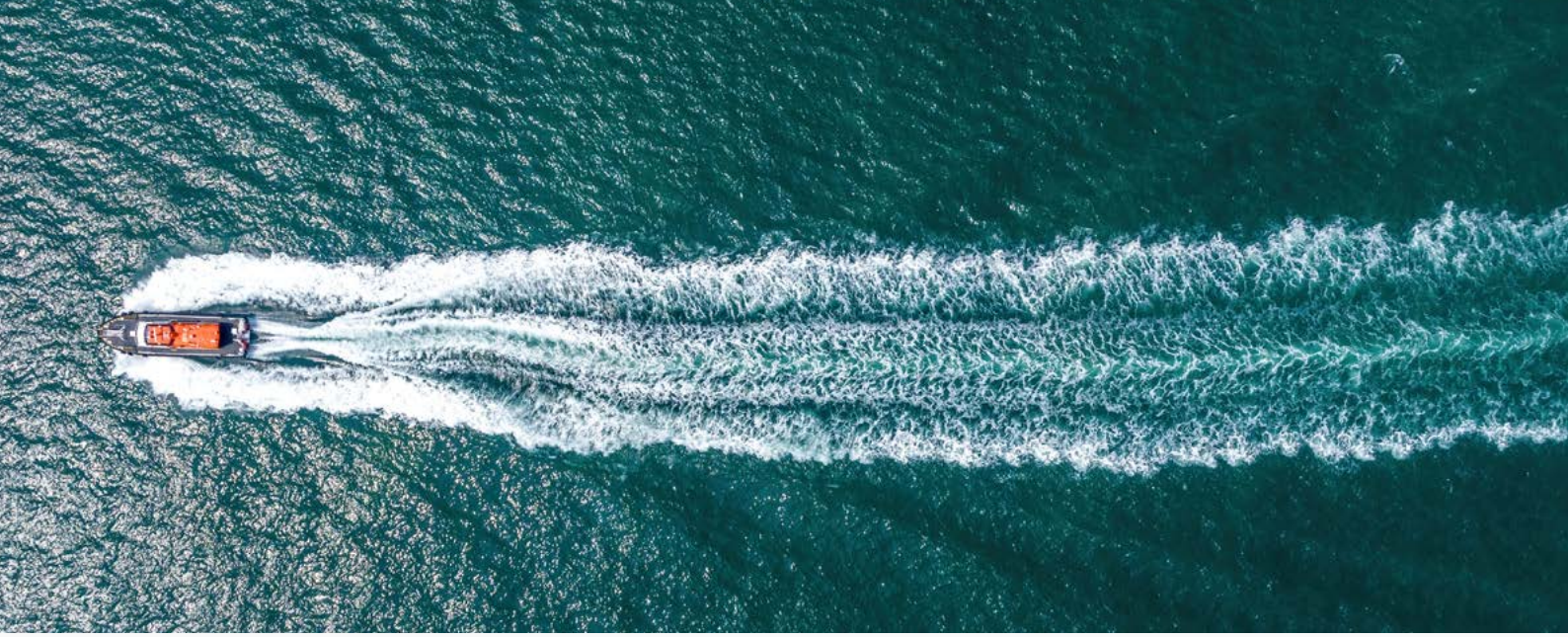
uvance Wayfinders

Consulting by Fujitsu

Australia's cyber divide:

Resilience in the age of AI

FUJITSU



How leading organsations are moving from compliance to continuous accountability

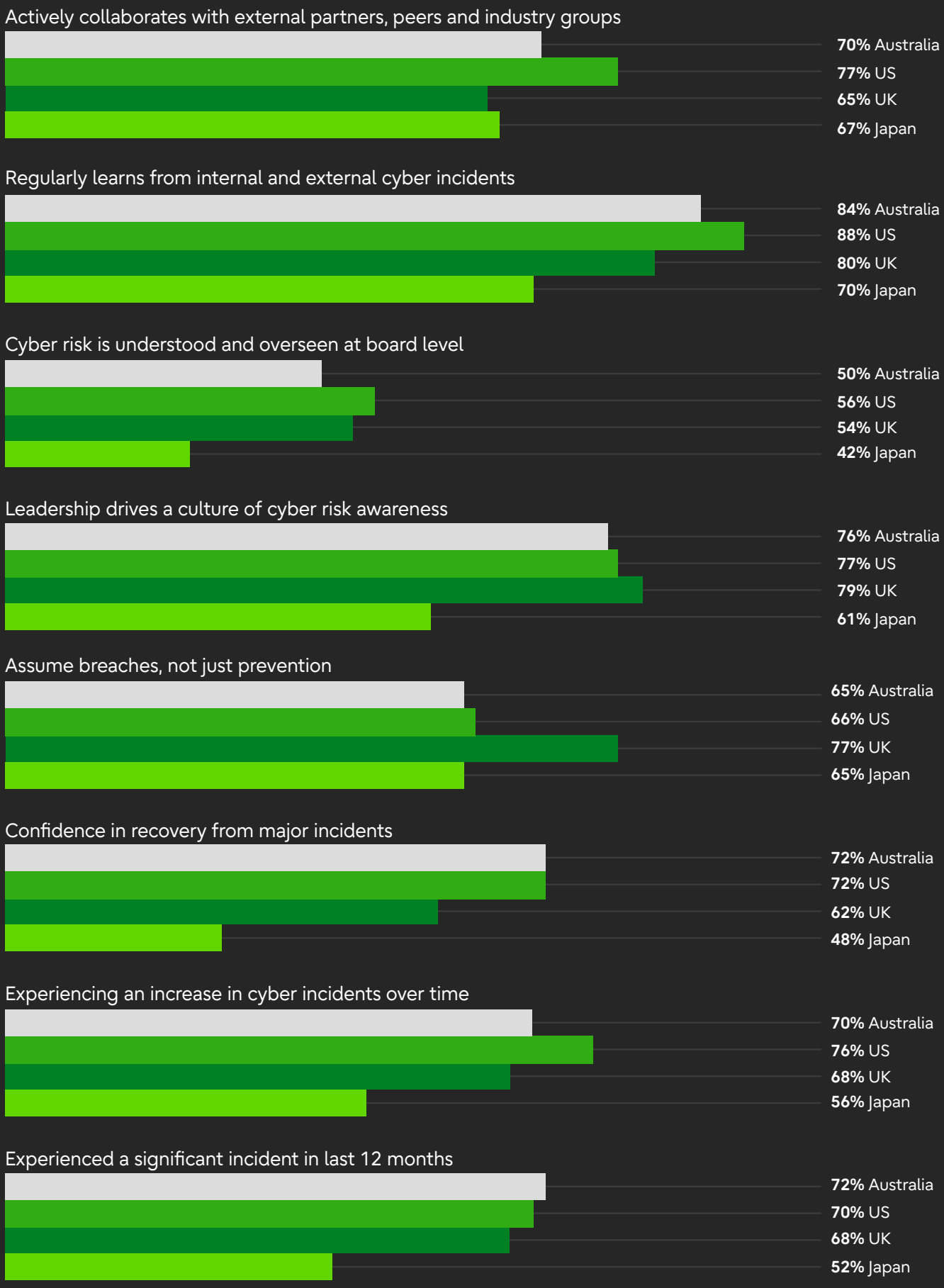
Australian organisations are operating in a cyber environment defined by speed, scale, and compounding complexity. Artificial intelligence is amplifying this reality in both directions: it is accelerating digital transformation, automation, and new customer experiences, while simultaneously enabling attackers to automate reconnaissance, craft increasingly sophisticated social engineering attacks and exploit human and process weaknesses at a pace that traditional security controls struggle to match.

New Uvance Wayfinders research signals that cyber disruption is no longer a rare or isolated IT issues. Our new global survey, inclusive of 100 Australian executives shows it is a repeatable operational risk with direct implications for service continuity, trust, and organisational performance. Nearly three-quarters (72%) of Australian executives report their organisation experienced at least one significant cyber security incident in the last 12 months. A majority report a higher number of incidents compared with three years ago. The key question for leaders has therefore shifted: not whether to be compliant, but whether the organisation can continue operating and making confident decisions when disruption inevitably occurs.

In that context, compliance should be treated as an uplift opportunity rather than a finish line. When approached well, regulatory obligations and standards can drive better governance, clearer ownership, improved evidence of control effectiveness, and more consistent risk decisions across the enterprise. When approached poorly, they become box-ticking exercises that divert scarce budget and attention away from the risks that matter most.

The purpose of this report is to translate the data into practical, business-led priorities for CISOs and CIOs: how to build continuous cyber accountability, strengthen assurance, and enable AI adoption with confidence.

Figure 1: Australia's cyber resilience posture vs global peers



Q1: To what extent do you agree with the following statements about your organisation's cyber resilience?
Footnote: Total respondents n= 400

Australia's cyber risk reality

Australia's cyber risk profile reflects both high digital adoption and concentrated exposure across critical infrastructure, regulated industries, and the public sector. Energy networks, healthcare systems, transport, financial services, and government services are increasingly interconnected, increasing the attack surface and raising the real-world consequences of disruption.

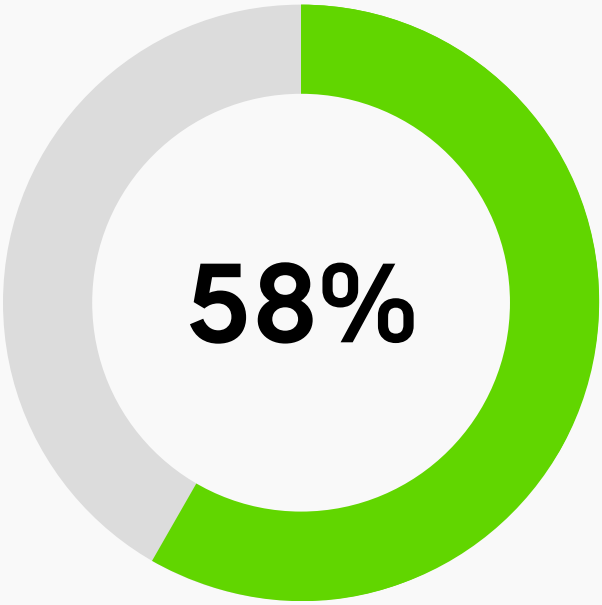
The research indicates Australian organisations are among the most affected in the study, reporting both high incident frequency and increasing concern about adversary capability. For CISOs and CIOs, this combination creates sustained pressure: security teams must respond to more events, while executives and boards need stronger assurance that risk statements, control ratings, and third-party reports reflect reality.

AI is accelerating the shift. Automated tools allow attackers to identify vulnerabilities faster and exploit weaknesses almost immediately to gain access to key assets and systems. For organisations with complex supply chains, distributed workforces, and legacy platforms, response windows compress and the operational impact of even brief cyber outages grows. The expanding scope of what is considered 'critical', through regulation, customer requirements, and interdependence means more organisations must now demonstrate resilience, not just intent.

The dual challenge: External threats and internal complexity

Cyber risk is now shaped by two pressures that reinforce each other. Externally, threats are faster, more automated, and harder to attribute, particularly as adversaries use AI to industrialise attack workflows. Internally, the technology environment is expanding as AI tools, data platforms, SaaS applications, and digital services proliferate across business units.

Many Australian leaders acknowledge that adoption is outpacing oversight. Unmanaged or "shadow" AI tools and models used without formal approval have emerged as a prominent concern.

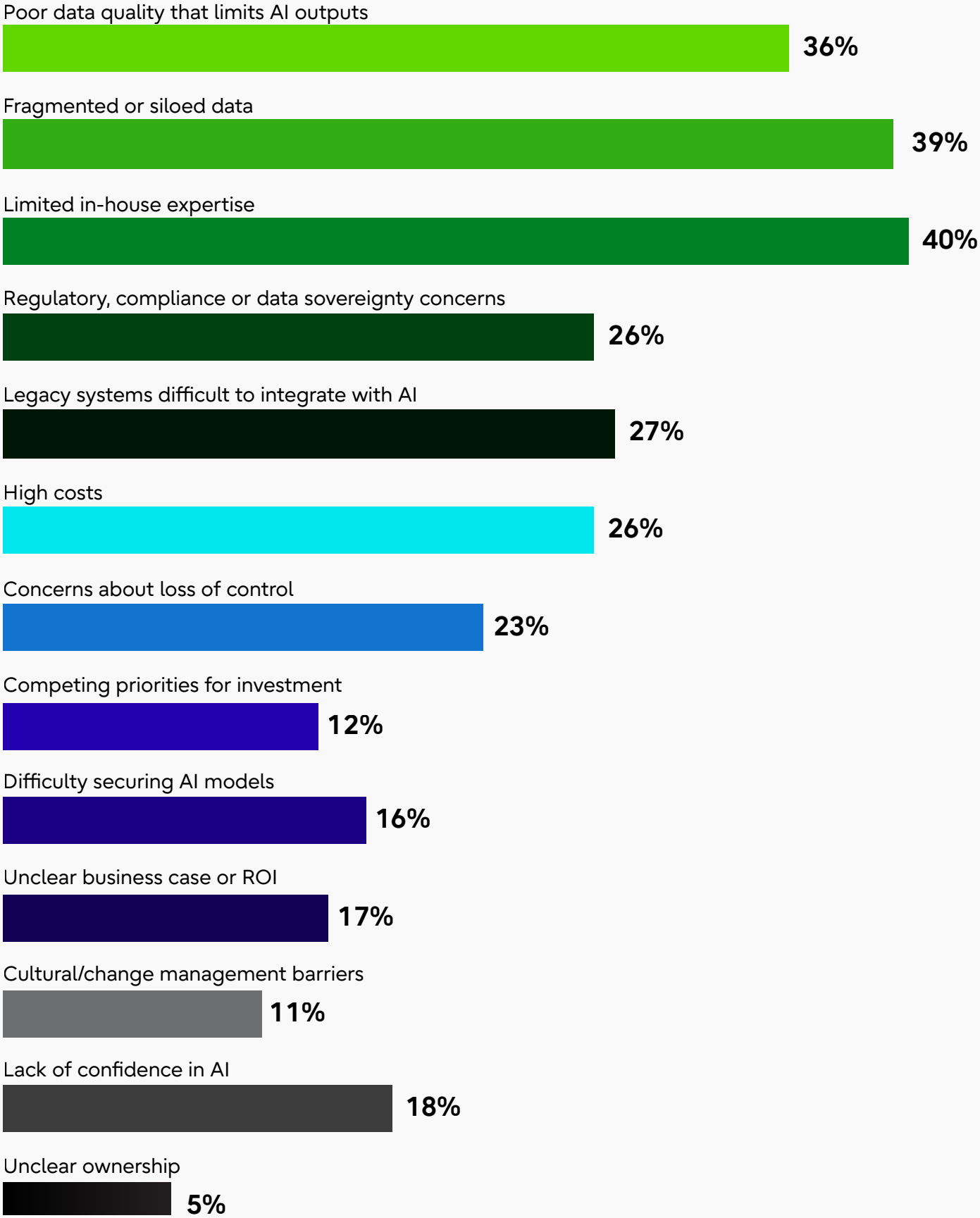


of Australian executives identify shadow AI as a growing cyber risk.

Without visibility as to where AI is being used, organisations cannot consistently apply security controls, manage data exposure, or maintain compliance with regulatory and ethical obligations.

Data foundations compound the challenge. Fragmented, siloed, or poor-quality data limits the effectiveness of AI-driven security tools, while skills shortages make it difficult to operationalise advanced capabilities at scale. In federated organisations such as government and large enterprises, risk increases further when policies and data maturity differ across business units. The outcome is a widening gap between organisations that can confidently govern AI-enabled risk and those that remain reactive, discovering exposures only after they become visible through audit findings, supplier incidents, or operational disruption.

Figure 2: What's holding Australia back from AI-enabled resilience? Data issues and skill gaps limit AI adoption



Q: Thinking about your organisation, what are the greatest barriers to embedding AI into cyber resilience strategies?
Footnote: Australian respondents n= 100

From prevention to operational resilience

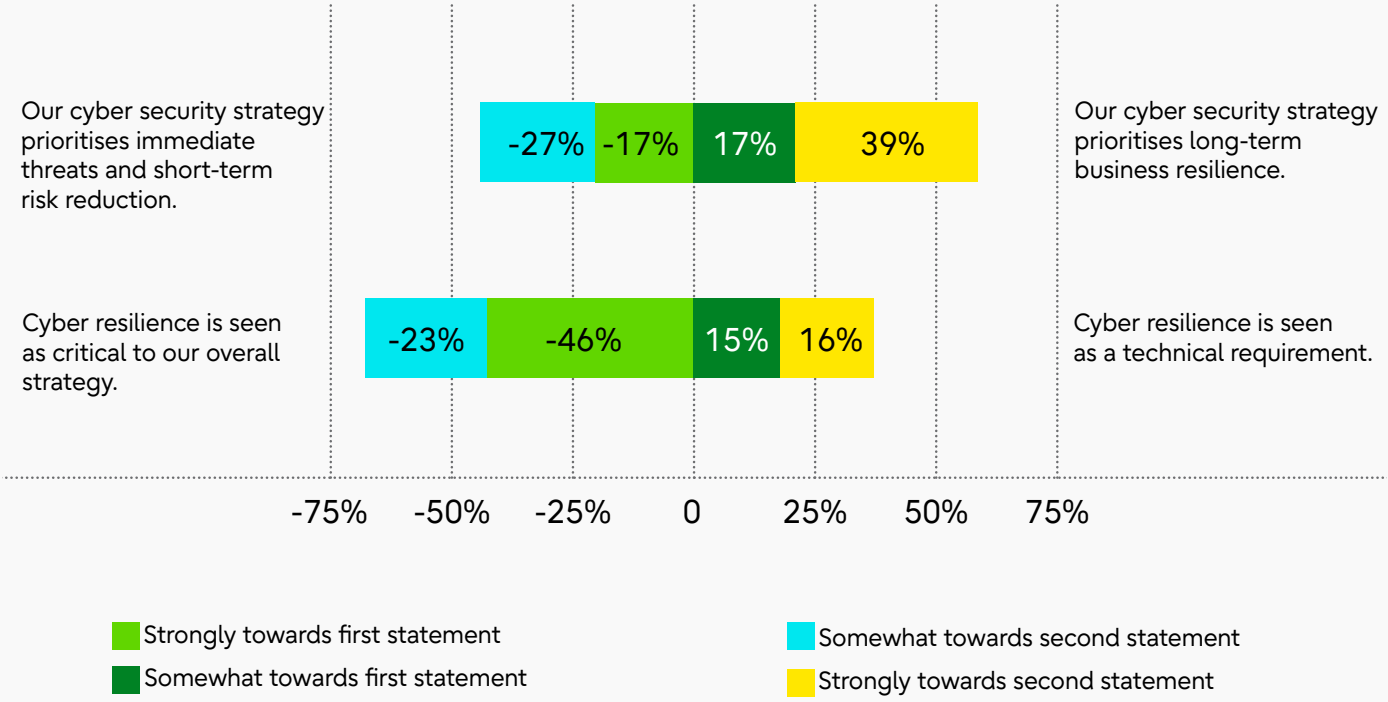
Traditional cyber strategies prioritised prevention: keeping attackers out. Prevention remains necessary, but it is no longer sufficient in an environment of advanced, persistent threats and AI-enabled acceleration. The research shows a decisive shift toward resilience-led thinking, with many Australian leaders indicating their strategy assumes breaches will occur (Figure 1). This is not pessimism it is operational realism.

2/3 **of companies report experiencing at least one significant cyber security incident in the past 12 months.**

However, confidence is uneven. Around two-thirds of leaders express confidence their organisation could withstand a major incident without significant commercial damage, while others remain concerned about prolonged outages, cascading supply-chain impacts, and loss of trust with customers, citizens, and regulators.

What separates these groups is less about sector or size and more about strategic intent: resilience is designed, funded, rehearsed, and measured against mission-critical services rather than assumed to exist because controls are documented.

Figure 3: Australia's resilience posture and strategic trade-offs



Q5: Thinking about your organisation's approach to future cyber resilience, which of the following statements best describes your situation?
Footnote: Australian respondents n= 100

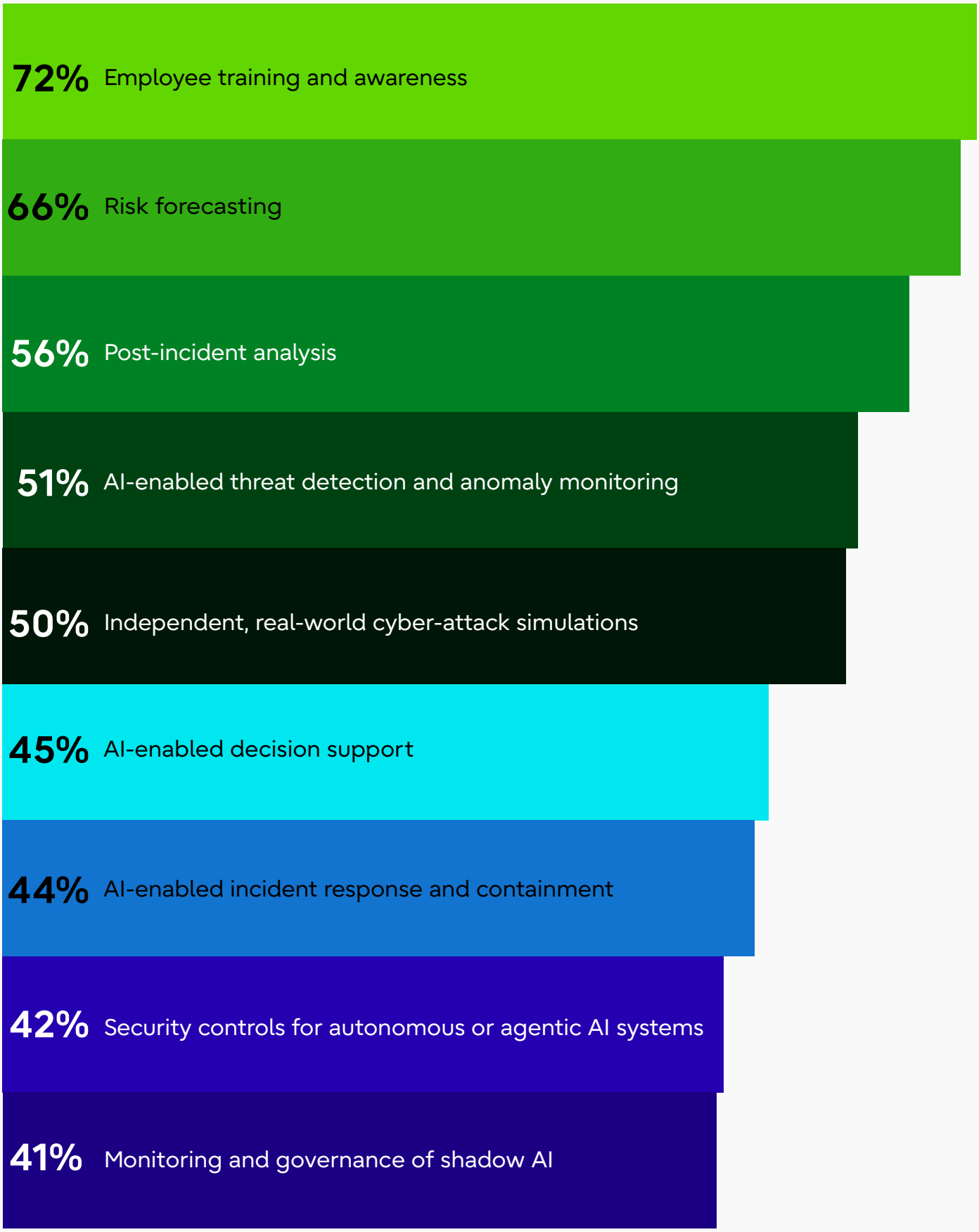
Leadership, culture and governance

Cyber resilience is as much a leadership challenge as it is a technical one. Organisations that perform strongly treat cyber risk as a board-level and executive responsibility, not something delegated entirely to IT or the security function. That governance model depends on translation: risk must be expressed in the language of business outcomes, service continuity, safety, customer trust, legal exposure, and strategic trade-offs, so that leaders can make informed decisions about investment and acceptance.

Culture follows leadership behaviour. Where executives promote awareness, learning, and accountability, staff are more likely to recognise threats, report issue early, and adopt secure practices. Where cyber is framed as a specialist concern, resilience becomes brittle and dependent on controls and a small number of experts, and vulnerable to surprises when business conditions change.

Governance must also avoid a common trap: mistaking compliance for risk reduction. Standards and regulatory obligations matter, but they do not automatically reflect an organisation's specific threat model, technology stack, or supplier dependencies. A value-led approach uses compliance to strengthen disciplines, control ownership, evidence quality, testing cadence, and reporting integrity while still prioritising investment toward the pathways most likely to cause business disruption. This is the essence of continuous cyber accountability: a living system of governance and assurance that evolves as the enterprise and threat environment evolve.

Figure 4: What resilience looks like in practice
Organisations are struggling to operate within the AI ecosystem



Q2: To what extent does your company use* the following solutions/initiatives to enhance cyber resilience?
Footnote: Australian respondents n= 100

AI as both risk and defensive advantage

AI is raising the stakes for cyber security, but it is also becoming one of the most powerful tools available to defenders. Australian leaders recognise this duality. AI-enabled attacks are cited as the top risk to organisational security and resilience today (61%), yet a strong majority also believe AI is becoming essential to defending against increasingly sophisticated attacks (67%). The practical implication is that organisations need an explicit position on AI: where it will be adopted, what guardrails apply, and how it will be used to strengthen security outcomes.

Defensive value does not come from tools alone. Without strong data foundations, clear model governance, and the skills to operationalise detection and response, AI-driven security can underperform or introduce new risk. The organisations extracting the most value treat AI security as part of a broader resilience strategy: they align telemetry to the services that matter most, define escalation paths that match business impact, and validate performance through exercises that reflect modern attack methods.

Figure 5: AI is amplifying both risk and defensive advantage peers

Q3: To what extent do you agree with the following statements about AI's role in cyber security?
Footnote: Total respondents n= 400

The business case for cyber resilience in Australia

The research establishes a clear link between cyber resilience and broader organisational outcomes. More resilient organisations are more likely to report positive performance across productivity, innovation, and trust not because cyber is a revenue function, but because disruption is a performance constraint. When leaders can rely on service continuity, data integrity, and effective recovery, they can make faster decisions, run leaner operations, and adopt new technology with fewer avoidable delays.

Strong cyber and AI security frameworks are increasingly viewed as enablers. In Australia, 61% of leaders say strong cyber resilience enables the development of new AI-enabled products and services.

The signal for CISOs and CIOs is important: investment cases land more effectively when they are tied to business value, speed-to-market, safe data use, and operational confidence rather than framed purely as technical risk avoidance. as a security capability.

Resilience also underpins trust.
Nearly seven in ten Australian leaders link strong AI security frameworks to building trust with customers and partners.
Trust is sustained not only by preventing incidents, but by demonstrating preparedness for when incidents occur: clear accountability, credible reporting, transparent communication during disruption, and strong supplier oversight.
In sectors where public confidence is foundational such as government, healthcare, energy, and other essential services, resilience is a legitimacy capability as much as a security capability.

Practical priorities for Australian leaders

The path to stronger cyber resilience is becoming clearer. Across the research and current operating realities, several priorities consistently distinguish organisations that can operate through disruption:

1. **Design for breach, not just prevention**

   Assume cyber incidents will happen. Define recovery objectives for critical services, engineer containment pathways, ensure decision rights are clear under pressure, and test recovery through exercises to ensure the organisation can restore operations effectively.

2. **Make accountability continuous**

   Use compliance as an uplift mechanism: assign control owners, improve evidence quality, test controls on a cadence, and ensure reporting reflects operational reality across the whole organisation, not just policy intent.

3. **Prioritise what matters most**

   Protect mission-critical services and high-value data flows rather than trying to defend everything equally. Link controls to the business processes they safeguard.

4. **Govern AI deliberately**

   Reduce shadow AI by creating approved pathways, data handling rules, and model governance that business units can actually follow. Treat AI use cases as risk decisions, not just technology deployments.

5. **Strengthen third-party assurance**

   Map critical supplier dependencies, validate their controls, and plan for supplier-driven disruption. Focus on measurable outcomes (availability, recovery, notification SLAs) rather than marketing claims.

6. **Rehearse the hard scenarios**

   Stress-test incident response through simulations that include AI-enabled social engineering, credential compromise, and supply chain impacts. Use lessons learned to update playbooks and governance

7. **Translate cyber into executive decisions**

   Report in terms of business risk. Enable boards and executive teams to understand where cyber risk is accepted, where it is mitigated, and what investment is required to address unacceptable risk levels.

Conclusion

Australian organisations are at a defining moment in their cyber resilience journey. AI is reshaping opportunity and risk at the same time, compressing response windows and increasing the consequences of failure. In this environment, cyber resilience is not an add-on to technology, it is a core operating capability that enables confident execution.

The research makes one point clear: incidents are no longer exceptional, and prevention alone is no longer sufficient. Organisations that align leadership around business outcomes, treat compliance as a lever for continuous accountability, and invest in AI-enabled defence as part of an end-to-end resilience strategy are better positioned to protect operations, people, and trust. For CISOs and CIOs, the objective is not perfect control, but it is credible assurance and sustained confidence: the ability to innovate, serve, and operate through uncertainty in an increasingly AI-driven world.

About the research

In February 2026, Uvance Wayfinders surveyed 400 senior business leaders based in Australia, Japan, the UK and the US. They represented technology and IT, finance, strategy and operations equally and were from companies across the following sectors: financial services; manufacturing; energy, resources and utilities; logistics and supply chain; retail and consumer goods; healthcare and life sciences; the public sector, government and defense; technology and telecommunications; and professional services. About half (53%) of companies had between 1,000 and 4,999 employees, 20% had between 5,000 and 9,999 employees and 28% had more than 10,000 employees. Percentages throughout this report may not sum precisely due to rounding.

uvance Wayfinders

Consulting by Fujitsu

Explore Uvance Wayfinders

FUJITSU