pwc

From risk to enabler

Australian insights on cybersecurity

Findings from PwC's 26th Global Digital Trust Insights 2024

Contents

Transforming cyber risks into business rewards

PwC's annual Global Digital Trust Insights 2024 survey demonstrates how digital market leaders are focussed on cyber integration to support business transformation and growth. They are responsive, agile and collaborative. In turn, their efforts yield fewer breaches and lower costs. But to thwart the ever-increasing threat of cyber adversaries, companies must accelerate their efforts to stay ahead.

Australian companies are confident their revenues will continue to rise in the year ahead (86%), but if they want to deliver on their optimistic expectations for growth, supported by digital transformation and AI, there's more they can do to see cybersecurity as an enabler and integrate it throughout business functions.

Business leaders should accelerate their current actions to match the level of risk and concern with integrated strategies, plans and continuous improvement. Against a backdrop of heightened awareness, companies increased budgets and lines of defence. Local organisations continue to experience costly breaches and these expenses are rising. More than one in three Australian organisations that experienced a data breach in the past three years reported costs of between $1.57 million and $14.2 million. One in 50 suffered breach-related costs of more than $31.7 million.

The Australian experience is distinct from our neighbours in the Asia-Pacific region and those globally. This is, in part, shaped by our regulatory environment, which is catching up to the rest of the world notably in critical industries. The 2023-2030 Australian Cyber Security Strategy will enhance regulations, secure government systems, build frameworks to respond to major incidents, and strengthen our international strategy. Australia cannot act alone on cyber. Everyone is impacted - and responsible - for cybersecurity.

PwC's 26th Global Digital Trust Insights 2024 highlights the priorities of Australia's business leaders. The survey reveals how focused leadership, coupled with strategic planning and resources can deliver significant benefits and mitigate risks. Backed by experience, these insights transform cyber risks into business rewards.

Australia at a glance

Australia's organisations are **most concerned** about attacks on connected devices and cloud-related threats.

49%
of respondents are most concerned about loss of customer, employee or transaction data.

33%
of respondents cited the board as their top engagement stakeholder. Almost one in three (31%) report to their CIO and 18% report to their CEO.

Key indicators

44%
of businesses will prioritise digital and technological risk mitigation this year.

74%
of Australian business leaders plan to increase their cyber budget in the year ahead compared to 60% in 2023.

55%
will increase their cyber budget between 6% and 14%.

The two main cybersecurity investment priorities over the next 12 months are application security 38% and cloud security 35%.

Points of interest

Threats posed by third party breaches are of greater concern in Australia (28%) than globally (23%).

Over the next 12 months, Australian organisations are more concerned about the loss of intellectual property (35%) than their global peers (26%).

46% of Australian organisations currently use technology solutions from multiple providers but are moving towards an integrated suite of solutions in the next two years.

Best-practice optimised and continuous improvement practices to establish a cross-functional resilience team are in place at 30% of Australian workplaces (25% global).

Australian organisations have also mapped their technology dependencies more effectively (31% compared to 24%).

Threats and opportunities

Cyber risks are top of mind

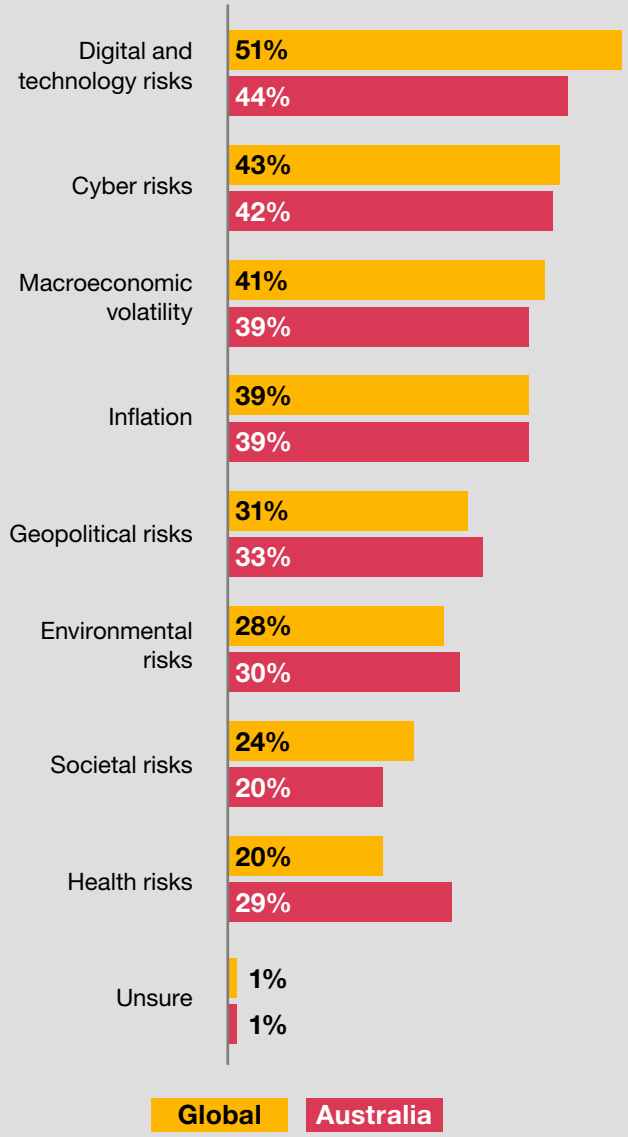
With Australian governance frameworks in place, the next step initiated by cyber leaders is to assess and monitor risks. The far-reaching impact of cyber incidents includes the loss of trust, reputational damage and financial losses. So, it is understandable that the potential outcomes of most concern from a cyber attack were loss of customers, employee or transaction data, loss of revenue, and brand damage (including loss of customer confidence). Damage to products or services and a loss of intellectual property were also significant concerns.

Then there are the direct costs. The self-reported cost of the most significant data breaches in the past three years was higher in many cases for Australian companies than those elsewhere. About two in three local organisations (64%) suffered between $158,000 to $14.2 million in losses.

Given the high-profile nature of recent cyber incidents due to ransomware, it may be surprising that this threat is ranked outside the top three for Australian respondents, while cloud-related threats, attacks on connected devices and hack-and-leak operations formed the top three reported concerns. Corporate leaders recognise the interconnected dependencies between companies and their value chains. From a cybersecurity perspective, companies are putting supply chain and third-party risk front and centre, a prudent measure given an organisation is only as strong as its weakest link.

Comparing our results to those internationally, Australian companies share similar priorities: digital and technology risks, cyber risks, and inflation. However, global respondents overall reported macroeconomic volatility above inflation risk.

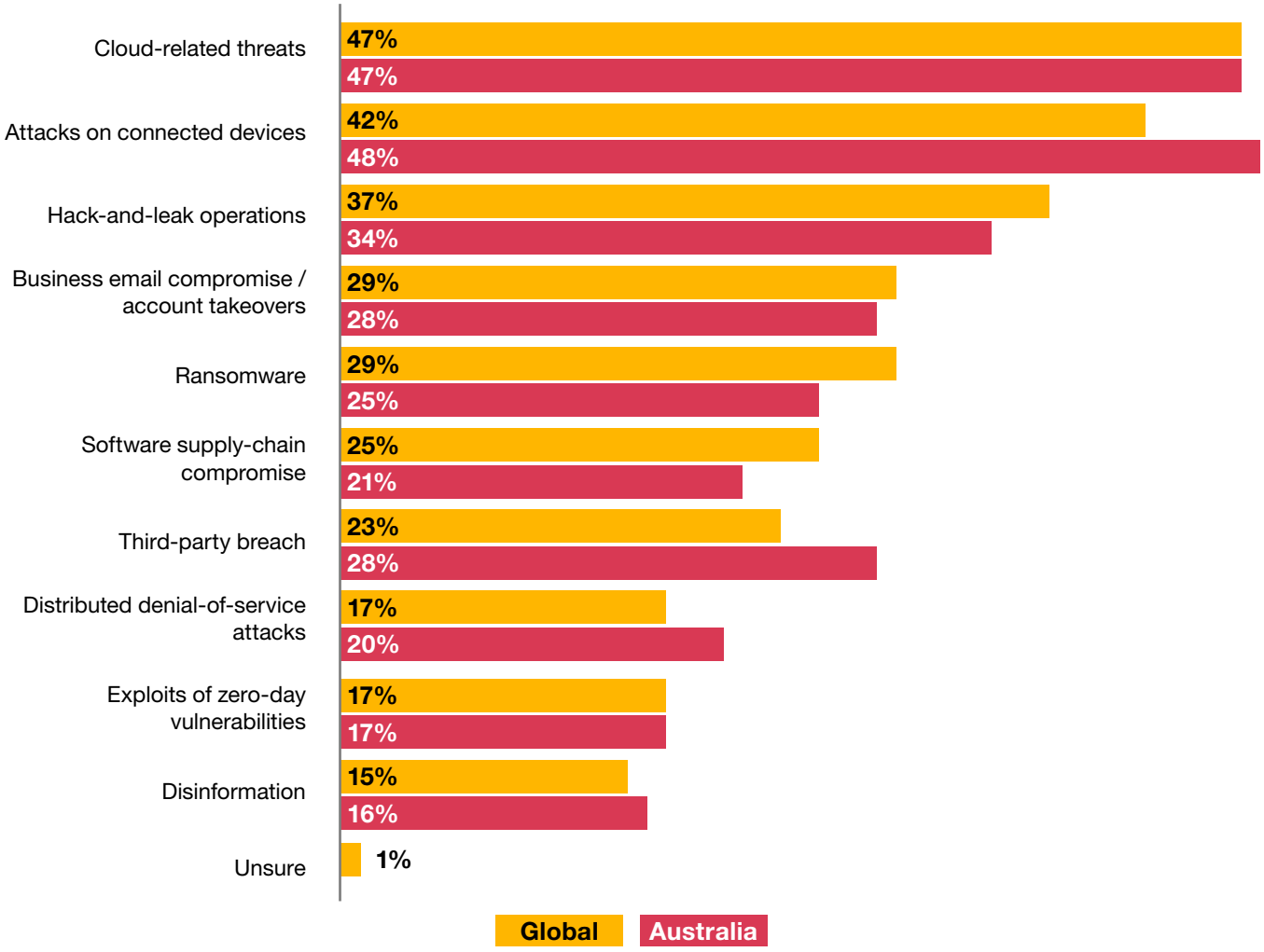
Organisation's risk mitigation priorities over the next 12 months



Question: Which of the following risks is your organisation prioritising for mitigation over the next 12 months? (Ranked in top three).

Base: Global = 3876, Australia = 122
Source: PwC, 2024 Global Digital Trust Insights.

Top cyber threats to organisations over the next 12 months



Question: Over the next 12 months, which of the following cyber threats is your organisation most concerned about? (Ranked in top three).

Base: Global = 3876, Australia = 122
Source: PwC, 2024 Global Digital Trust Insights.

Generative AI: emerging opportunities and risks

Breakthroughs in generative AI (GenAI) and large language models (LLMs) are setting records for the rate of adoption and reliance on AI within organisations.

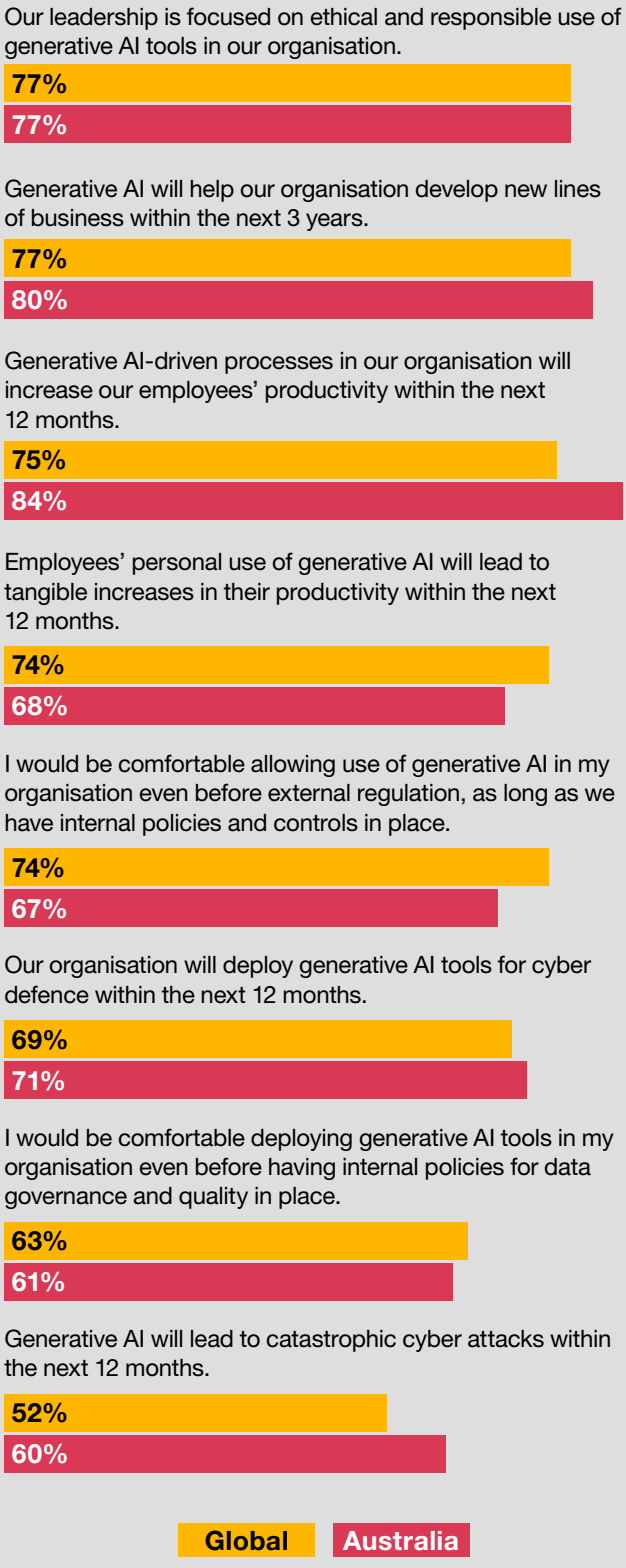
Conversational AI user interfaces, embedded AI in third party software and cloud-based 'auto ML' tools, mean today's AI landscape is no longer constrained to data scientists, software engineers and the major technology vendors. Across virtually every industry, organisations are exploring GenAI use for everything from productivity, new products and services, customer experience, quality and cyber risk management.

The advantages are already being realised. One in five (21%) of Australian businesses are benefiting from GenAI and LLMs to detect and mitigate cyber threats. Worldwide, approximately seven out of 10 organisations are preparing to use GenAI in their cyber defence.

Australians are optimistic about GenAI opportunities. Four out of five (80%) believe it will help to develop new lines of business in the next three years. Most believe generative AI-driven processes will increase employee productivity within the next 12 months (84%). From this positive mindset, a majority (67%) are willing to proceed with the use of GenAI before external regulation, subject to internal policies and controls. Conversely, business leaders also have a degree of caution with concerns over costs associated with increasing AI regulation and business transformation.

A majority (60%) of Australian respondents agreed or strongly agreed the technology will lead to 'catastrophic cyber attacks' within the next 12 months. And yet, the anxiety is not matched by action. Just 37% have included and continually update the risks of GenAI in their cyber plan. To develop the potential of GenAI, business leaders must educate themselves and establish safeguards to protect their operations and business from cyber threats.

To what extent do you agree or disagree with the following statements about Generative AI?
(Those who selected 'Strongly agree' or 'Agree').



Question: To what extent do you agree or disagree with the following statements about Generative AI? (Those who selected 'Strongly agree' or 'Agree').

Base: Global = 3876, Australia = 122
Source: PwC, 2024 Global Digital Trust Insights.

Response

Budgets are getting bigger

Cybersecurity budgets are being raised. Companies are taking into account the rising threats and regulatory settings and recognise the need for greater investment. Far more local organisations are increasing budgets in 2024 compared to in 2023, in response to well publicised breaches. A quarter of respondents (24%) expect to increase their cyber funding by more than 11%. Another 34% will lift their budgets from between 6% to 10%. But there is tension between the business and technology leaders as to where to spend it.

Funding priorities for Australian business leaders for 2024

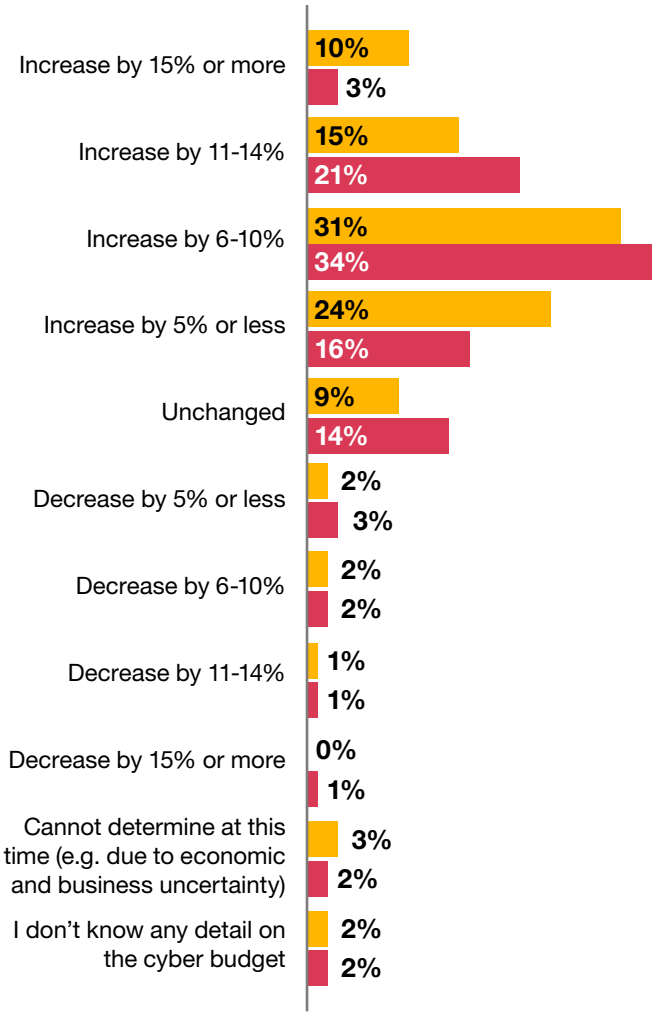
- Modernisation of technology, including cyber infrastructure
- Ongoing improvements in risk posture based on cyber roadmap
- Ongoing security training
- Compliance with regulations or directives

Funding priorities for Australian technology leaders for 2024

- Application security
- IoT security
- Cloud security
- Managed security services

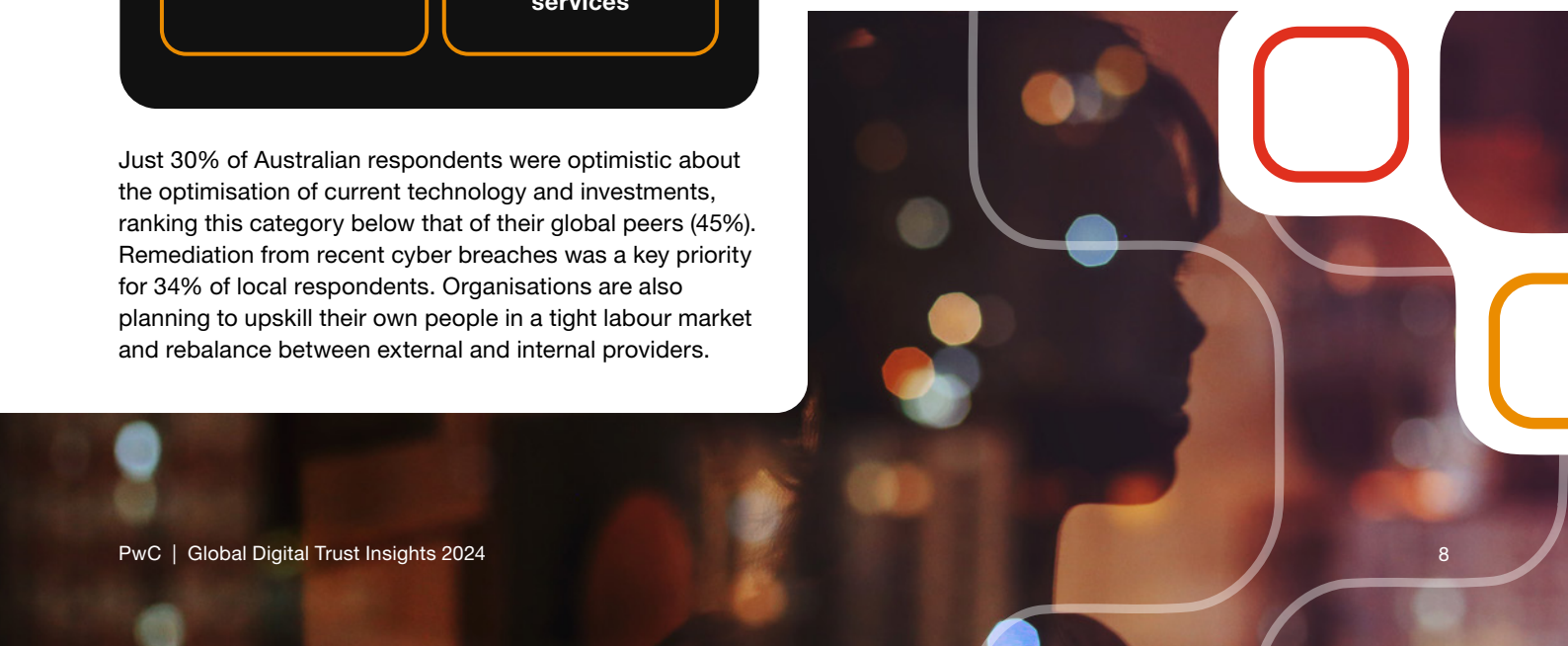
Just 30% of Australian respondents were optimistic about the optimisation of current technology and investments, ranking this category below that of their global peers (45%). Remediation from recent cyber breaches was a key priority for 34% of local respondents. Organisations are also planning to upskill their own people in a tight labour market and rebalance between external and internal providers.

Changes to cyber budgets in 2024



Question: How is your organisation's cyber budget changing in 2024?

Base: Global = 3876, Australia = 122
Source: PwC, 2024 Global Digital Trust Insights.

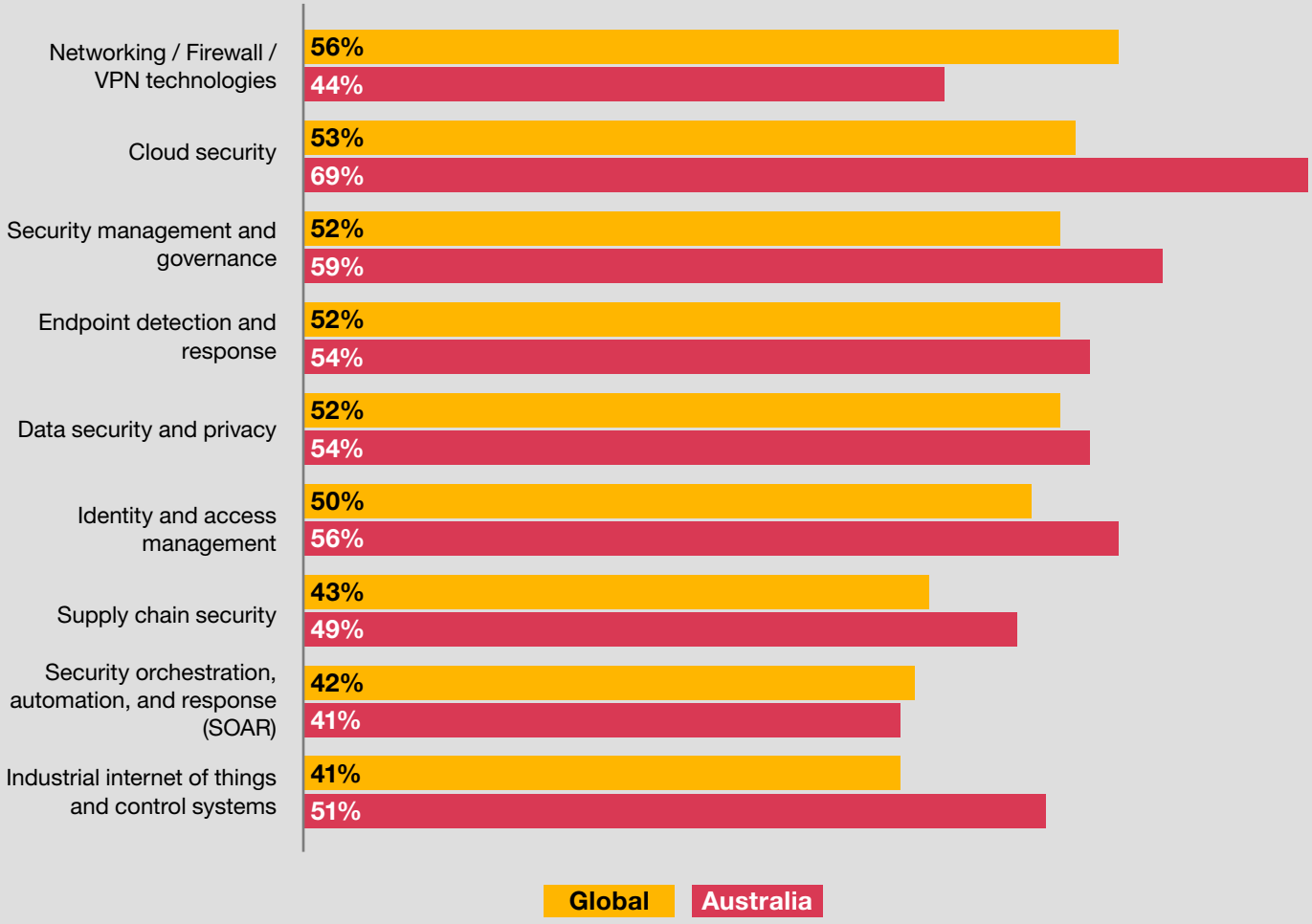


Are organisations satisfied with their cyber investments?

Despite increased budgets, companies are not wholly satisfied with their capabilities in cybersecurity. Locally, we continue to build resilience through investments. As Australian companies mature, there is an opportunity to focus on holistic business enablers - including recovery systems - over and above resilience settings. In an escalating threat environment, proactively anticipating future cyber risks will be essential to reap the full benefits of a cyber secure organisation. One in five Australian organisations (21%) are already realising benefits from LLMs or GenAI for risk detection and mitigation. Another 31% have used the systems but are yet to see the payoff.

Australian organisations are content with their security management and governance (59% very satisfied), which aligns with the reporting to organisational leadership. Likewise, they are quite confident about their capabilities in endpoint detection and response (54%), data security and privacy (54%) and identity and access management (56%).

Organisations that are 'very satisfied' with their technology capabilities



Question: How satisfied are you with your organisation's technology capabilities in the following areas? (Those who are 'Very satisfied').

Base: Global = 1517, Australia = 39
Source: PwC, 2024 Global Digital Trust Insights.

Managing cloud security

Cloud is a key enabler to hyperscaling and business innovation, allowing operations to collaborate across borders and timezones. It is also backed by secure features. Major providers of cloud are investing significantly in their cybersecurity in order to support a superior service to clients. Despite these investments, uncertainty remains. Cloud security ranks high in budget allocation worldwide and in Australia (ranked in the top three for 33% global and 35% local respondents).

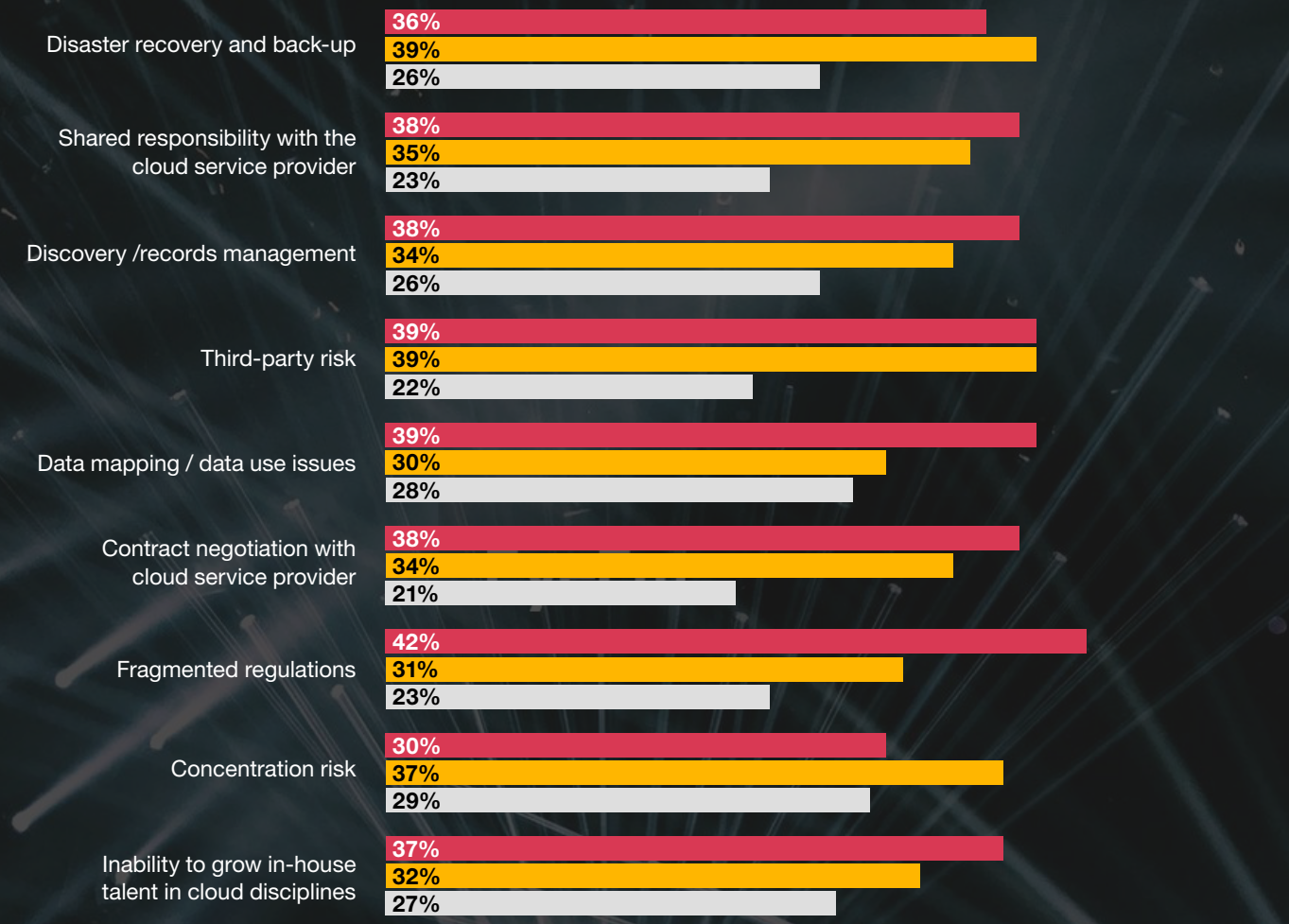
In Australia, most companies are using private and public cloud service providers or both. Just 8% store their data on premises. Local companies are significantly less likely to use the hybrid approach than internationally (33% to 42%). However, with the proliferation of 'shadow IT' and cloud-based apps, this lower reporting may be highlighting a lack of visibility over their tech locally.

Fewer than two in five companies have developed a plan for disaster recovery and back-up and continually update it.

A similar proportion have addressed shared responsibility, discovery and records management, third-party risk and data mapping with their cloud service provider. Fragmented regulations and concentration risk are also on their radar.

Overcoming these challenges requires a balance between finding an appropriately scalable and secure solution and reducing the attack surface from multiple providers. An accurate awareness of current tech platforms is essential, especially in regards to cybersecurity services which often evolve quickly. From there, technology rationalisation and consolidation can dramatically reduce security risks. If companies are leveraging the cloud, there's a good chance they are simplifying their technology environment and reducing their legacy tech footprint. This not only reduces complexity, but also leverages the benefits of cloud provider investments in security. Australian companies are more confident than those internationally (85% compared to 69%) that they have the right amount of cybersecurity technology solutions. Globally, organisations are twice as likely to report they have too many and want to consolidate (19% compared to 10%).

Organisation's position on cloud service provider challenges



Question: To what extent has your organisation addressed the following challenges with your cloud service provider(s)?

Base: Global = 3648, Australia = 111
Source: PwC, 2024 Global Digital Trust Insights.

Governance and reporting lines

Australia is still in catch-up mode on cyber regulation compared to global jurisdictions. But as the rollout of the expanded Security Legislation Amendment (Critical Infrastructure Protection) Act progresses, the onus is on those critical industries to oversee and manage threats. Directors are on notice that effective plans must be in place, along with mandatory reporting requirements, by August 2024. For financial APRA-regulated entities, boards will bear the responsibility for reporting obligations under the CPS 234 Information Security standard. In this context, Australian cyber teams report to their boards much more frequently than overseas (33%). Alternatively, cyber teams report to the Chief Information Officer (31%) or the CEO (18%).

More regulation is expected and Australian entities are already factoring in significant increased costs from harmonised cyber and data protection laws and increased regulatory requirements for operational resilience.

The survey reveals one in five Australian company cyber teams bring their insights on risk exposure and mitigation measures to the CEO and board. But there is a clear opportunity for improvement if more organisations communicate their cyber awareness and understanding directly to their leaders. To be the key enablers of cyber - and business success - this communication loop is a critical and effective feedback process.

Boosting resilience

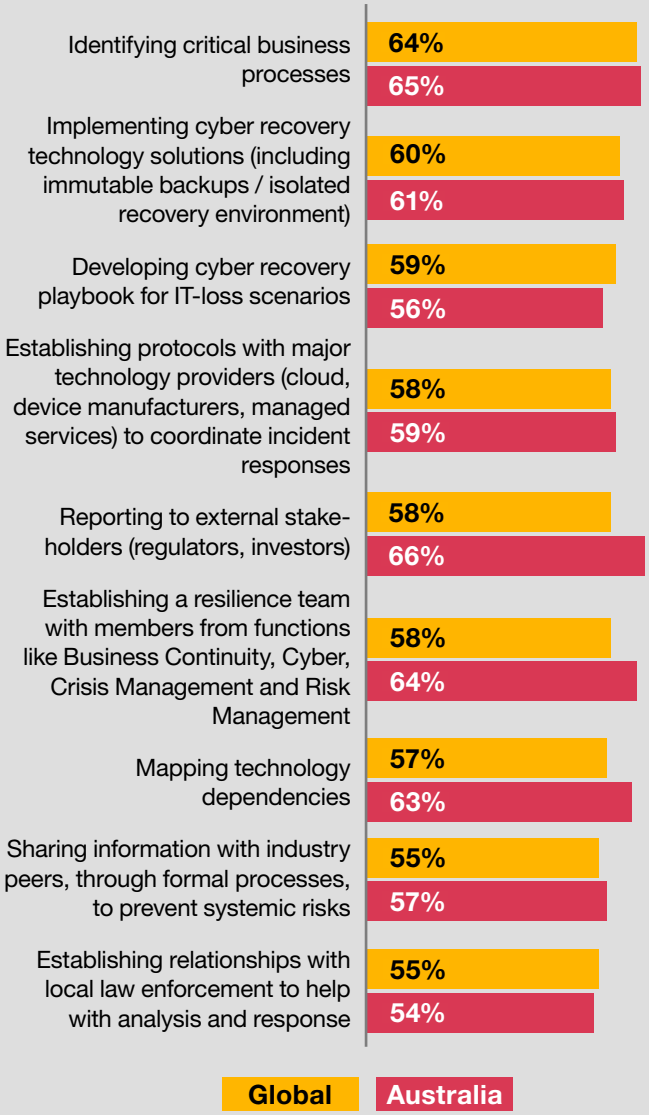
With governance structures and risk management in place, the focus is now on resilience. While protection and prevention are essential, there is recognition that breaches are inevitable. What matters is response and recovery. Recovery means having the confidence that operations can be broken down and built back up again. Leading organisations are building resilience for when the inevitable occurs.

In Australia, 65% of companies have identified critical business processes, consistent with global peers (65%). Likely due to recent regulatory changes, 66% of local companies have systems to report to external stakeholders, higher than internationally (58%), and sharing information with industry peers through formal processes (57% Australia, 55% globally). A majority of Australian organisations (64%) have established a resilience team with members from functions including business continuity, cyber, crisis management and risk management.

For the next two years, organisations will focus on a number of resilience measures. These include developing a cyber recovery playbook for IT-loss scenarios (15%), establishing protocols with major technology providers (cloud, device manufacturers, managed services) to coordinate incident responses (11%), and reporting to external stakeholders such as regulators and investors (11%). In the shift to zero trust, Australian entities are putting a higher priority on software-defined access than those overseas (53% compared to 40%) to make it the highest ranked initiative. Secure endpoints and secure cloud networking are also critical.

To what extent is your organisation implementing or planning to implement the following cyber resilience actions? (Those who selected 'Optimised and continuous improvement').

Question: To what extent is your organisation implementing or planning to implement the following cyber resilience actions?
(Those who selected 'Implemented across the organisation' and 'Optimised and continuous improvement').



Question: To what extent is your organisation implementing or planning to implement the following cyber resilience actions? (Those who selected 'Implemented across the organisation' and 'Optimised and continuous improvement').
Base: Global = 3876, Australia = 122 | Source: PwC, 2024 Global Digital Trust Insights.

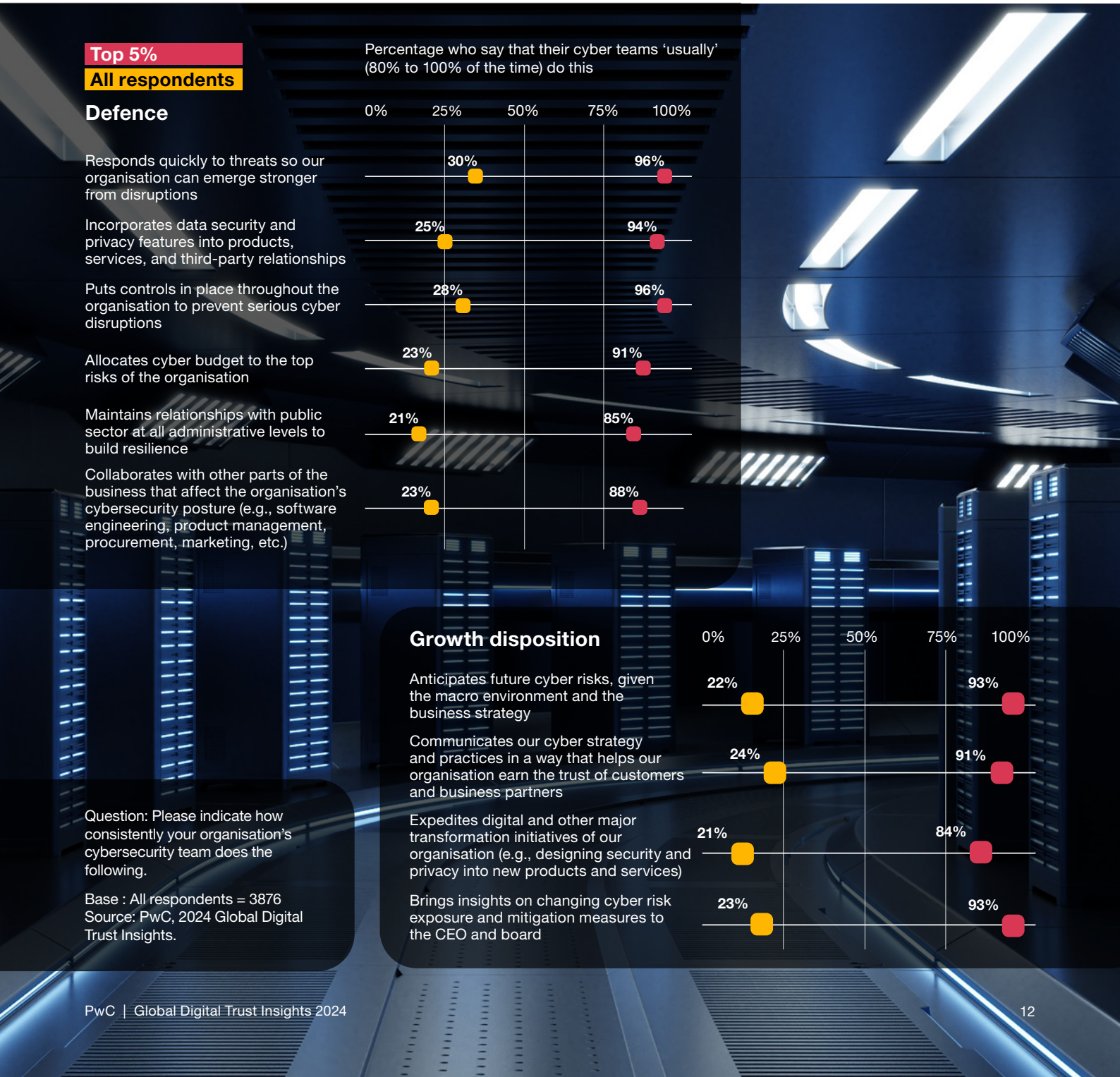
Cybersecurity as an enabler

Global top performers

A small group of companies have moved beyond cyber resilience to cyber excellence. We call them our stewards of digital trust. This cohort have integrated security and cyber at the centre of innovation, where opportunities are developed, defended and protected.

These businesses are reaping benefits others are missing, are more than likely to be high growth, and their cyber leaders report to the board or CEO. In these top performing organisations, the CISO is at the forefront of business, supported by an accelerated budget, with continually updated cyber practices embedded throughout the business.

Worldwide, 179 organisations achieved stewardship of digital trust. It's not just about security and defence. It's about benefits, too. The top 5% experience fewer breaches and when they do occur, they're far less costly.



Question: Please indicate how consistently your organisation's cybersecurity team does the following.

Base : All respondents = 3876
Source: PwC, 2024 Global Digital Trust Insights.

Global top performers vs the rest

Top 5% are

6x more likely to have already implemented transformative cybersecurity initiatives from which they are realising benefits.

5x
more likely to be very satisfied with their current cyber technology capabilities.

4x
more likely to be continually updating their risk management plan to mitigate cloud risks.

9x
more likely to be mature in their cyber resilience practices.

Top 5% are more likely to

Invest more into cyber budget, with 85% increasing their cyber budget in 2024 (vs 79% overall), of which 19% are increasing cyber budget in 2024 by 15% or more, compared to 10% overall.

Say their most damaging cyber breach in the past three years cost them less than $158,000 (28% vs 19% overall).

Strongly agree their organisation will develop new lines of business using generative AI (GenAI) (49% vs 33% overall).

Plan to deploy GenAI tools for cyber defence (44% vs 27%).

Disagree that 'GenAI will lead to a catastrophic cyber attack' (33% vs 22% overall).

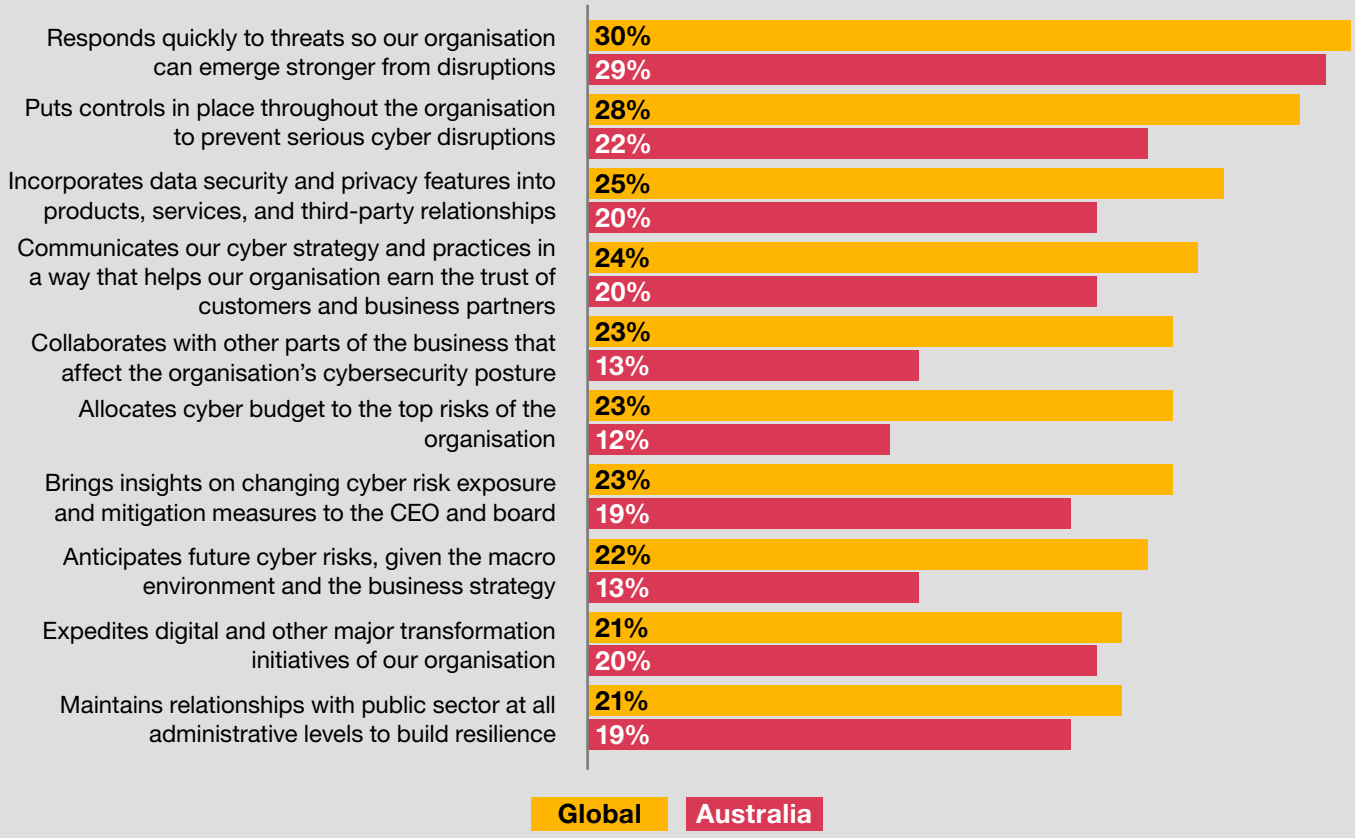
Ready to respond?

Despite current efforts in governance, risk and operations, more work is needed. Cyber teams still need to be better integrated into the business, to allow for greater information sharing and collaboration. This is where Australian companies don't fare as well as those globally. There is a marked difference in responses regarding cyber teams collaborating with other parts of the business that affect the organisation's cybersecurity posture (13% Australia and 23% global), and allocating cyber budget to the top risks of the organisation (12% versus 23%).

Although local companies are responding quickly to threats and putting controls in place throughout the organisation to prevent serious cyber disruptions (22% versus 28%), there is room for improvement.

Cyber should be harnessed as an opportunity. Through collaboration and the integration of cyber expertise into all aspects of the business, costs can be reduced and risks mitigated. Further, secure digital systems offer new revenue streams or enhance existing products and services. Our global top performers demonstrate that the transformation of cyber from a risk to a critical enabler can be done successfully.

Please indicate how consistently your organisation's cybersecurity team does the following
(Those who selected 'Usually (81-100% of the time').



Question: Please indicate how consistently your organisation's cybersecurity team does the following.
(Those who selected 'Usually (81-100% of the time').

Base: Global = 3876, Australia = 122
Source: PwC, 2024 Global Digital Trust Insights.

Global Digital Trust Insights 2024 methods

The DTI survey received 3876 responses globally, including 122 participants from Australia. There were 71 territories represented and a range of industry sectors and organisation sizes.

Globally, sectors included industrial manufacturing (20%), financial services (20%), technology, media and telecommunications (19%), retail and consumer (17%), energy, utilities and resources (11%), healthcare (9%), and government and public services (3%). Of these, 43% had revenues of more than $10bn. One-quarter were publicly listed, while 30% were privately owned with backing from private equity.

PwC asked core questions for all job roles, and added additional queries for those in security and IT roles (CIO, CSO, CTO, Cybersecurity Director, Information Security Director, Information Technology Director).

Contact us to learn more

Robert Di Pietro
Cybersecurity & Digital Trust Leader
robert.di.pietro@au.pwc.com

D0623034