



# Cyber and the C-suite in Australia

Findings from 2023 Global Digital Trust Insights Survey





## Executive summary

### Global insights, uniquely Australian perspectives.

Around the world, digital transformation continues to drive business innovation, diversification and post-pandemic regeneration. We are more connected than ever before, which has fundamentally changed the way we work, the systems that underpin the everyday and the way we view security. Cybersecurity is now

central to almost all organisational operations – it is the backbone of business. And while Australia too, has been swept up in the shift to digitisation, the way our CISOs and the C-suite view this rapid transformation is distinct, as this report shows.

There are two key factors we believe have contributed to these uniquely Australian perspectives.

The first is our geographical isolation, the world's largest island nation and a near-neighbour of Asia. While a great strength, the COVID-19 pandemic showed that our isolation can create significant supply chain issues, the ramifications of which continue to be felt.

And second, over the past several years, Australia's cyber-related legislative and regulatory landscape has evolved quickly. In particular, significant reforms to the critical infrastructure regime, which has seen the number of captured sectors expand from four to 11, has meant many organisations have had to fundamentally change the way they view cybersecurity, rebuilding from the ground up.

But the goalposts keep moving. Cyber is not static.

Rapid digitisation means cybersecurity has to be everyone's business. It cannot be siloed within organisations, which needs to involve all parts of the

business in getting cyber right. As we race towards a future that promises more connected systems and exponentially more data, we will face more strategic and sophisticated cyber adversaries.

With ever-expanding cyber risks, Australian business leaders have much more work to do. And the work has to be done in a tough economic environment where, more than ever before, consumers and shareholders demand cyber protections.

The findings from Australia's 2023 Global Digital Trust Insights Survey clearly show where our nation's C-suite have placed their cyber priorities, what their main concerns are and who bears responsibility for cyber across business functions.

It illustrates Australia's strengths, Australia's weaknesses and provides clear guideposts for the future – guideposts that will ultimately help our nation become more cyber secure.

# Australia at a glance

In 2023, the top two cyber threat actors expected to significantly impact organisations:

Cyber criminals



Insider threat

Since 2020, Australian organisations have experienced:



Increased exposure to cyber attacks due to increased digitisation



Increased demand for disclosure of cyber incidents and practices



Heightened regulatory investigations or enforcement action or litigation

## Key indicators

**60%** of Australian organisations will increase their cyber budget in 2023

**25%** will increase cyber budget by 6-10%

**28%** of respondents said cyber budgets would remain unchanged

**90%** of respondents expected the government to develop cyber techniques for the private sector, based on the knowledge base built from mandatory disclosures of cyber incidents

**88%** of respondents reported they could provide the required information about a material or significant incident within the required reporting period after the incident

## Top five: Scenarios being incorporated into organisational resilience plans



Global recession



Supply chain bottlenecks



Catastrophic cyber attack



Commodity market volatility



Significant workforce churn

## Points of interest:

Threats posed by software supply chain compromise were of much greater concern to Australian respondents (**37%**) than globally (**26%**)

**81%** of Australian respondents felt new requirements for mandatory disclosures of cyber incidents to investors or national cyber authorities would discourage sharing information with law enforcement (**64% globally**)

**90%** of Australian respondents reported public information sharing and transparency was a risk that could lead to a loss of competitive advantage (**70% globally**)

Australian organisations are more reactive in their approach to cyber disruption, with **63%** (**47% globally**) invoking plans post-incident and focussing on recovery and remediation. Just **37%** (**53% globally**) reported taking an anticipatory and preventative approach by assuming incidents will occur and embedding mitigations accordingly

Australian organisations have been slower to promote integrated and agile operating models that can respond to a diverse set of disruptive events (**30%**; **40% globally**), and are more likely to use individual, pre-defined plans and processes designed for responding to specific disruptions (**70%**; **53% globally**)

**Demographic snapshot:** 104 – the number of Australians that completed the survey | \***69%** of respondents were from organisations with annual revenue more than US\$1billion | **70%** male; **30%** female | **65%** business executives; **35%** tech executives | **38%** of respondents were from organisations backed by private equity; **26%** were from a partnership

\*3522 surveys were completed globally

# Threat actors

As digitisation bounds forward, creating new opportunities and efficiencies for business, there is a downside – just like there are gains to be had for business, cyber threat actors have also leveraged digitisation.

Australia’s C-suite put cyber criminals at the top of the list of threat actors most likely to significantly affect their organisation in 2023 (67%), in line with global trends (65%). However, unlike their global counterparts, Australian respondents also expect insider threats and competitors to present a significant challenge (58% and 57%; 44% and 42% global).

Third-party providers (46%), web applications (44%) and mobile devices (43%) were reported as the top three pathways adversaries would use to gain access to business systems in 2023, with the key threat vectors predicted to be attacks against cloud management

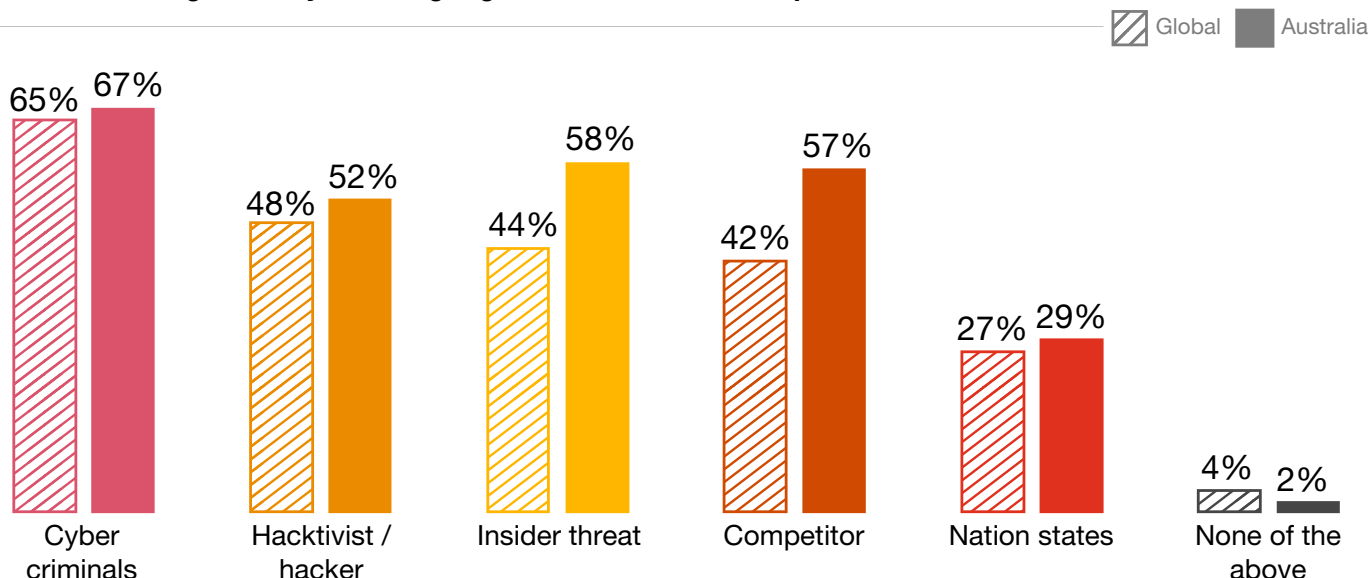
interfaces (39%), software supply chain compromise (37%), intellectual property theft for commercialisation (33%), and attacks on industrial internet of things (IIoT) or operational technology (OT) (33%).

It is interesting to note that threats posed by software supply chain compromise were of much greater concern to Australian respondents (37%) than they were globally, where only 26% of respondents saw this vector as a significant threat. This indicates that recent high-profile global attacks on software supply chains, which had knock-on impacts domestically, have left Australian respondents on high alert. It also reflects Australia’s pandemic hangover, which has heightened concerns about supply chain security and ultimately played catalyst to significant critical infrastructure reforms.

## Top five threat actors, vectors and attacks Australian organisations are least prepared to address

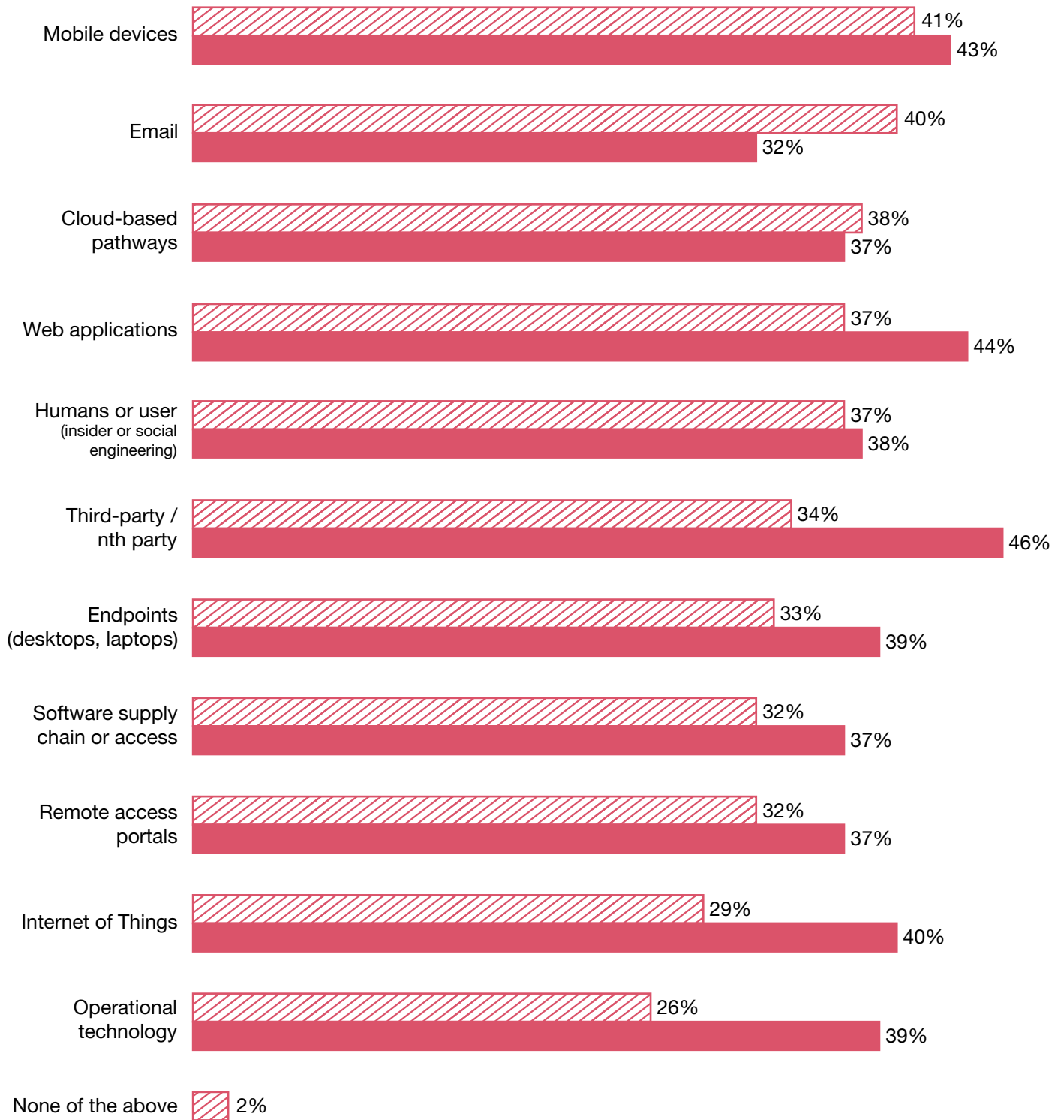
- 1 Cyber criminals
- 2 Hacktivist / hacker
- 3 Insider threat
- 4 Competitor
- 5 Third-party

## Threat actors significantly affecting organisations in 2023 compared to 2022



Question: For each of the threat actors below, which do you expect to significantly affect your organisation in 2023 compared to 2022?  
 Base: Global=3522, Australia=105 Source: PwC’s Global Digital Trust Insights Survey 2023, Final Results, September 2022.

## Pathways that adversaries will significantly affect organisations



Australia Global

Question: For each of the pathways by which adversaries can gain access to your systems, please select those that you expect to significantly affect your organisation in 2023 compared to 2022.

Base: Global=3522, Australia=105

Source: PwC's Global Digital Trust Insights Survey 2023, Final Results, September 2022.

# Who are Australia's cybersecurity decision makers?

As the old adage goes, cybersecurity is a shared responsibility. This saying is being put into practice by Australia's C-suite, who are sharing the load across the diverse range of business functions and decisions that cyber touches.

While CISOs and CIOs retain most key cyber responsibilities, CEOs, CFOs and CDOs were well represented across all areas. While Australian results did not differ substantially from global results, one point of departure was in relation to managing data governance and privacy, with the majority of Australian respondents (22%) reporting the CEO bore this responsibility. Globally, the CIO (16%) and the CDO (15%) were viewed as the responsible stakeholders in this area.

## Reporting on cyber and privacy risks to the board and senior management\*

Global	Australia
CISO 21%	CIO 25%
CIO 16%	CEO 18%
CEO 13%	CISO 13%
CFO 7%	CFO 10%

## Managing third-party risks\*

Global	Australia
CISO 18%	CIO 18%
CIO 15%	CEO 15%
CEO 12%	CFO 10%
CRO 10%	CISO 10%

## Deciding on cyber budget\*

Global	Australia
CFO 20%	CEO 19%
CEO 17%	CIO 17%
CIO 14%	CFO 13%
CISO 14%	CISO 12%

## Cyber due diligence of M&A target\*

Global	Australia
CISO 17%	CIO 29%
CIO 17%	CEO 24%
CEO 13%	CISO 13%
CFO 8%	CDO 10%

## Coordination on cyber incident response\*

Global	Australia
CISO 25%	CISO 21%
CIO 17%	CEO 16%
CEO 11%	CFO 14%
CDO 8%	CIO 14%

## Managing data governance and privacy\*

Global	Australia
CIO 16%	CEO 22%
CDO 15%	CISO 16%
CISO 15%	CDO 12%
CEO 12%	CIO/CPO 10%

\*CISO and top three responses shown  
 Question: Who is primarily responsible for each of the following areas of cybersecurity within your organisation? Base: Global=3522, Australia=105 CISO and top three roles shown.  
 Source: PwC's Global Digital Trust Insights Survey 2023, Final Results, September 2022.



# Communicating with key stakeholders

In relation to communicating cyber to priority stakeholders, Australia presented an anomaly, with the top three targets over the next year ranked as CEOs, regulators for consumer protection and value chain participants. In what was a key point of departure, boards ranked first globally but fifth in Australia.

This result is surprising given the key role boards must play in setting the cyber agenda, as well as the increasing responsibility Australian directors bear under regulation in relation to cyber posture. Therefore, it is advisable Australia's C-suite engage better with their boards, and make this engagement a priority.

## Why Australian boards need to be across cybersecurity

Significant reforms to secure Australia's critical infrastructure are now in force, entailing specific obligations requiring the attention of boards. It is essential directors understand the intent of the reforms, how the legislation requires certain enforceable activities to be undertaken and how to prepare for managing compliance and building critical infrastructure resilience. These reforms have occurred against a backdrop of regulatory complexity. For example, Australian Prudential Regulation Authority's (APRA) prudential standards CPS 234 Information Security (and proposed CPS 230 Operational Risk Management) has created enhanced obligations for APRA-regulated entities, with boards bearing ultimate responsibility.

## How to help boards

C-suite can help boards get savvy about the cybersecurity of their organisation. Some key ways to improve cyber reporting to boards are:

- Presenting a scorecard/dashboard that helps board members understand the key cyber risks to the organisation with relevant metrics
- Explaining the organisation's cybersecurity strategy and how it is aligned with the organisation's overall strategy
- Familiarising them with the business continuity, contingency and recovery plans so they are prepared to act quickly in the event of a cyber incident

## What boards can do

- Make sure adequate time is allotted to the CISO and cyber-related matters at meetings
- Don't settle for substandard board reporting – demand meaningful information and the insights required to instil confidence the organisation is managing its cyber risks
- Remember, cybersecurity is not an end state, so monitor how the company is making progress in its cyber posture and ability to defend against emerging threats
- Ask to take part in exercises that help you understand your organisation's cyber resilience



# Disclosures

## Ability to disclose cyber practices, strategy and incidents externally

As it comes to disclosing organisational cyber practices, strategy and incidents externally, Australian respondents are more confident than their global counterparts.

- **88%** reported they could provide the required information about a material or significant incident within the required reporting period after the incident (**81% globally**)
- **88%** reported can effectively assess the materiality of a cyber incident for the purposes of reporting (**80% globally**)
- **88%** reported they could describe the relevant cyber expertise on their board for the purposes of reporting (**78% globally**)
- **86%** reported their organisation has a policy stating which information can or cannot be disclosed regarding cyber incidents (**76% globally**)
- **86%** reported they could provide information about third-party cyber risk management (**75% globally**)

However, in an age of growing transparency, with consumers increasingly concerned about how their data is stored and used, domestic results indicate that Australia is lagging behind global counterparts.

Of particular concern were attitudes towards public information sharing and transparency, with **90%** of Australian respondents reporting it was a risk that could lead to a loss of competitive advantage (**70% globally**). Furthermore, **81%** felt new requirements for mandatory disclosures of cyber incidents to investors or national cyber authorities discourage us from sharing information with law enforcement authorities, compared to **64%** globally.

Eighty-nine per cent of Australian respondents agreed mandatory disclosures of cyber incidents requiring comparable and consistent formats were necessary to gain stakeholder trust and confidence (**79% globally**). In addition, organisations want government to help set standards, with **90%** of respondents stating they expected the government to develop cyber techniques for the private sector, based on the knowledge base built from mandatory disclosures of cyber incidents (**75% globally**).

### The new era of cyber transparency

Stakeholders clamour for more information about how companies manage their cyber risk exposure.

- Regulators want visibility into cyber practices because they want to protect citizens from fraud and loss of privacy, help investors make better decisions and prevent industry- or system-wide disruptions.
- Investors are looking for consistent and comparable disclosures so they can put their money in companies that fit their needs. Cyber incidents can affect shareholder value — temporarily or permanently.
- Individuals know their data and privacy are vulnerable to cyber breaches.
- Business partners want their data and other assets to be safe. These stakeholders want to understand how much they can trust in the ability of businesses and entire systems to withstand increasing cyber threats.

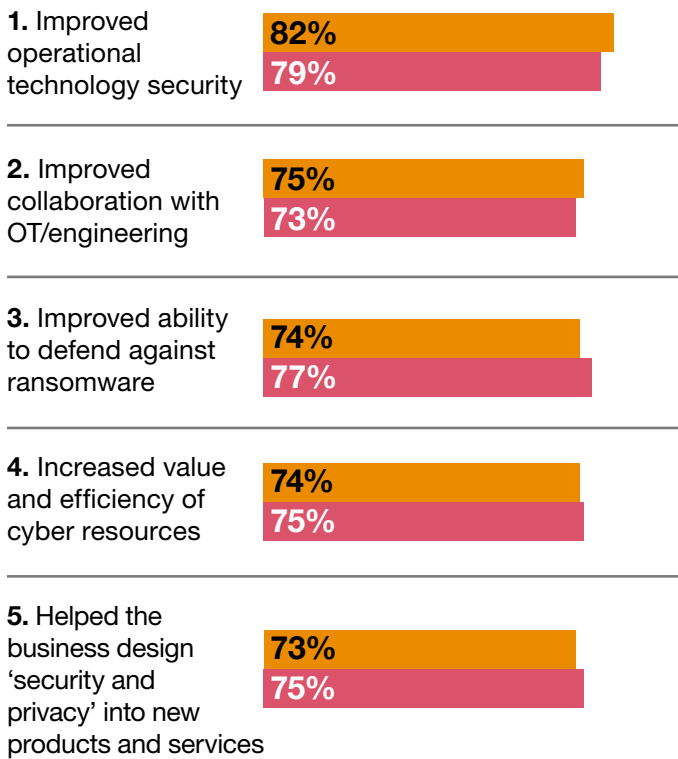




# Mitigations

Over the last year, Australian organisations have been focussed on mitigating cybersecurity risks associated with increased data volumes (**96%**); risks associated with increased supply chain digitisation (**95%**); and risks associated with launching new products and/or services (**95%**).

Australian CISOs and C-suite reported their top five cybersecurity accomplishments over the past year as:

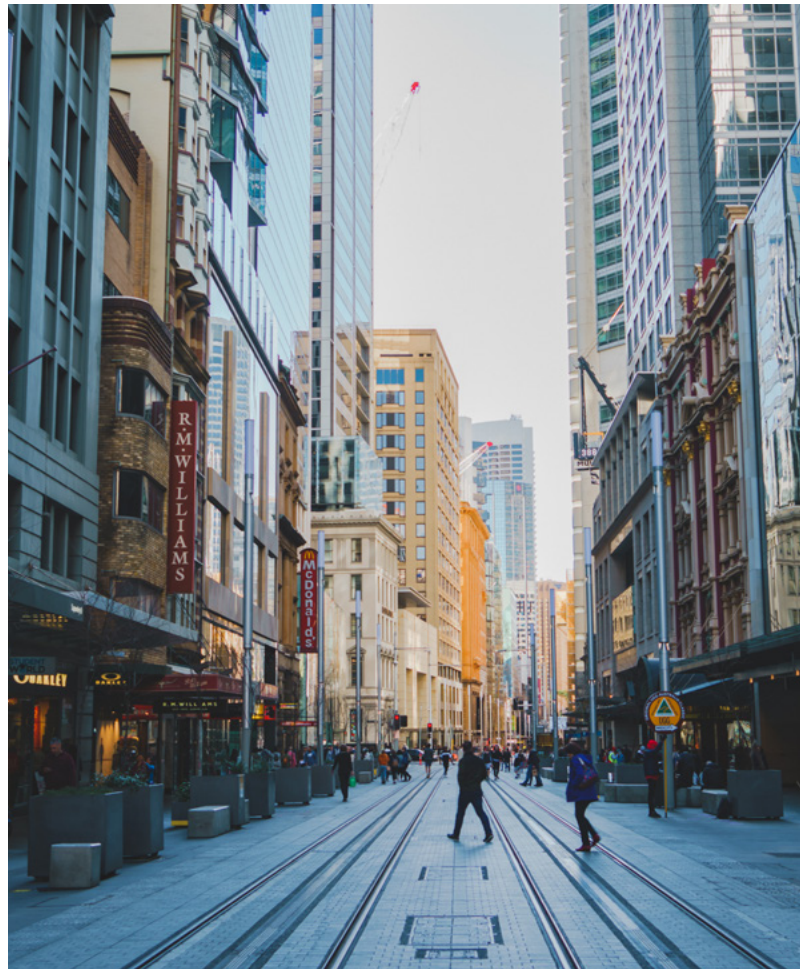


**KEY**  Australia  
 Globally

\*Top five responses shown  
 Question: Please indicate whether or not your organisation's cybersecurity team has accomplished the following in the past 12 months. Base: Global=3522, Australia=105.  
 Source: PwC's Global Digital Trust Insights Survey 2023, Final Results, September 2022.

While these steps are positive, improvement is required in several key areas where Australia is lagging behind global counterparts.

Outside the C-suite, Australian organisations need to get teams across different sections working better together, with **62%** reporting ineffective orchestration of cross-functional efforts to comply with new regulation (**70% globally**). They also need to better future-proof their organisations, with just **67%** reporting they were anticipating new cyber risks related to digital in initiatives before partners and customers were affected (**71% globally**).



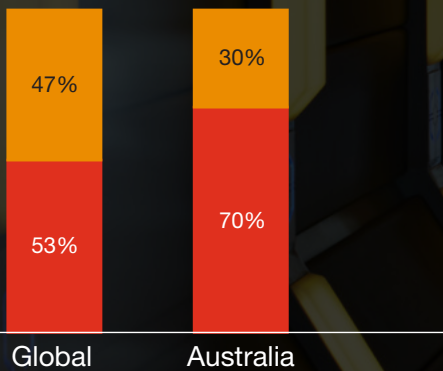
# Current cyber resilience approach and capability

## KEY OBSERVATIONS:

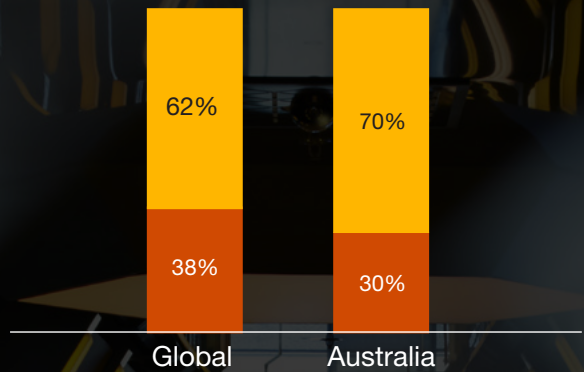
Like their global counterparts, Australian organisations are more focussed on developing a broad understanding of cyber risks and how to maintain business continuity (**70%**) than they are with isolated risk scenarios and how to tackle them (**30%**).

However, Australian organisations have been slower to promote integrated and agile operating models that can respond to a diverse set of disruptive events (**30%**; **47% globally**), and are more likely to use individual, pre-defined plans and processes designed for responding to specific disruptions (**70%**; **53% globally**).

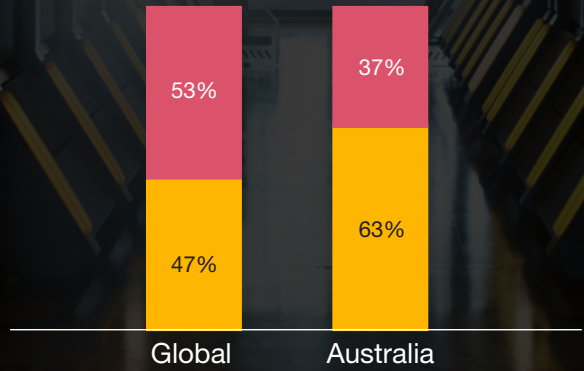
Furthermore, Australian organisations are more reactive in their approach to cyber disruption, with **63%** (**47% globally**) invoking plans post-incident and focussing on recovery and remediation. Just **37%** (**53% globally**) reported taking an anticipatory and preventative approach by assuming incidents will occur and embedding mitigations accordingly.



- Uses individual, pre-defined plans and processes designed for responding to specific disruptions
- Promotes an integrated and agile operating model that can respond to a diverse set of disruptive events



- Focuses on isolated risk scenarios and how to address recovery for that specific disruption
- Develops a broad understanding of risks that corporations now face, and how to continue operations amid simultaneous risks across the entire organisation



- Reacts to a disruption by invoking plans after an incident, and focusing on recovery to return to business operations after a failure or incident
- Takes an anticipatory and preventative approach by assuming that incidents will occur, and embedding resilience capability to withstand an occurring disruption

Question: For each of the following paired statements, which statement better describes your organisation's current cyber resilience approach and capability?  
 Base: Global=3522, Australia=105  
 Source: PwC's Global Digital Trust Insights Survey 2023, Final Results, September 2022.

# Driving uplift

For Australia’s C-suite, the top five factors that would help drive cybersecurity transformation in their organisations across the next 12-18 months are:






- 1 Leadership that drives cybersecurity throughout the organisation
- 2 Ensuring all non-cybersecurity employees understand the potential cyber implications of their actions
- 3 Strengthening data analytics capabilities on cyber and privacy activities
- 4 Educating the board on cyber risks
- 5 Solving the talent gaps in the cybersecurity workforce

This generally aligns with global results, with the only anomaly being that globally, consolidation of enterprise technology solutions for a simpler tech stack/ infrastructure was more pressing than solving talent gaps in the cybersecurity workforce.

However, when it comes to the top five scenarios being incorporated into organisational resilience plans, the difference in focus was stark. Globally, catastrophic cyber attack was the top scenario being considered for resilience planning, whereas in Australia, teams reported preparing for a global recession was top priority. Similarly, while inflation was a key focus globally, Australian respondents were more concerned with commodity market volatility, a sign of our economic reliance on natural resources.

These differences highlight that the Australian C-suite is highly attuned to the specific vulnerabilities our isolation could cause - that in the event of a global recession, we are more exposed to supply chain pressures and commodity market volatility, both of which could have devastating impacts on domestic industries and the labour market.

## Top five scenarios being incorporated into organisational resilience plans

Australia		Global	
1. Global recession		1. Catastrophic cyber attack	
2. Supply chain bottlenecks		2. Global recession	
3. Catastrophic cyber attack		3. COVID-19 resurgence or other health crisis	
4. Commodity market volatility		4. Inflationary environment	
5. Significant workforce churn		5. Supply chain bottlenecks	

# Dealing with data

Data is valuable to organisations and cyber criminals alike – some have called it the ‘new oil’ – and it is increasingly being commoditised. Australian businesses are becoming adept at using data to better understand what customers want and it is now part and parcel of customer-centric digital transformation.

However, to capture lasting value from this transformation, companies need to process and manage data and algorithms intelligently and efficiently. At the same time, security, ethical and privacy concerns need to be front and centre, in lock-step with regulatory compliance.

Recent high-profile data breaches have shown that more than ever before, customers expect that their data is effectively protected and, when it is no longer required, is not retained. Business must be alive to this trend, which will only become more important as Australia’s privacy regulation continues to tighten. Customer consent and privacy must be taken seriously.

## Top three: Policies, practices related to management and governance of customer data

Australia	Global
1. We follow an opt-in, privacy-first strategy in our marketing efforts (83%)	1. We only use customer data when we have express consent (79%)
2. We vet all the third parties and partners with whom we share customer data (82%)	2. New products and services go through a data security and privacy evaluation before launch (79%)
3. We use the newest techniques to pseudonymise our customers' data (81%)	3. We vet all the third parties and partners with whom we share customer data (78%)

## Top three: Inhibitors to organisational ability to use data for decision making

Australia	Global
1. <b>Accessibility:</b> The extent to which data can be accessed easily by authorised users	1. <b>Security and governance:</b> The extent to which the information is protected against theft, malicious manipulation and unauthorised access
2. <b>Security and governance:</b> The extent to which the information is protected against theft, malicious manipulation and unauthorised access	2. <b>Accessibility:</b> The extent to which data can be accessed easily by authorised users
3. <b>Usability:</b> The extent to which data is concisely presented and the ease with which it can be manipulated or processed	3. <b>Accuracy:</b> The extent to which there are no errors in the data



## Conclusion

While cybersecurity presents significant challenges for Australian organisations, it also offers opportunities. Building trust - with customers, the community and shareholders - is central to harnessing the opportunities presented by digital transformation, and creating a cybersecurity culture lies at its heart. This culture must be driven from the top, by the C-suite.

This report shows Australia's C-suite is on the right track but there is still a lot of work to do. And this work will inevitably be occurring against the backdrop of an evolving regulatory landscape, new and sophisticated threat vectors and budgetary constraints. Therefore, the key takeaway for our nation's C-suite when it comes to cyber must be to work smarter and hit the message home harder.

- Data protection must be top of mind, not a nice to have or viewed as a burden. Customers entrust organisations with their data and are increasingly concerned with how that data is protected. And more and more, shareholders will view cybersecurity as a key investment metric which, if not up to scratch, will see them talk with their feet.
- Communication has to lay at the heart of every cybersecurity strategy. Boards, consumers and the community expect transparency when it comes to cybersecurity, so good communication is key. For the C-suite, clear communication with boards is of utmost importance and should be prioritised.
- To be truly cybersecure, organisations must be agile. It is no longer good enough to be purely reactive in our cybersecurity responses. Central to risk management is taking an all-hazards perspective, responding with appropriate mitigations and anticipating new and emerging threats.
- Cyber is a team sport - it should not be siloed within departments or organisations. To build a truly inclusive and holistic cybersecurity culture, entire organisations must be taken on the transformation journey, which the C-suite should lead. Cybersecurity uplift must be expressed as an opportunity, not a burden, and ultimately a vehicle to help organisations achieve their goals.

# About the survey

The 2023 Global Digital Trust Insights is a survey of 3,522 business, technology, and security executives (CEOs, corporate directors, CFOs, CISOs, CIOs, and C-Suite officers) conducted in July and August 2022. Female executives make up 31% of the sample.

Fifty-two percent of respondents are executives in large companies (\$1 billion and above in revenues); 16% are in companies with \$10 billion or more in revenues. Respondents operate in a range of industries: Industrial manufacturing (24%), Tech, media, telecom (21%), Financial services (20%), Retail and consumer markets (18%), Energy, utilities, and resources (9%), Health (5%), and Government and public services (3%).

Respondents are based in various regions: Western Europe (31%), North America (28%), Asia Pacific (18%), Latin America (12%), Eastern Europe (5%), Africa (4%), and Middle East (3%).

The Global Digital Trust Insights Survey is formerly known as the Global State of Information Security Survey (GSISS).

PwC Research, PwC's global Centre of Excellence for market research and insight, conducted this survey.

## Australian respondents:

The total number of respondents from Australia was 105 executives. Of the Australian respondents, 65% were business executives while 35% were technology and security executives. Female executives made up 30% of the sample. Sixty-nine percent of Australian respondents are executives in large companies (\$US1 billion and greater in revenues); 31% are in companies with less than \$US1 billion.

Respondents operate under various ownership structures: 88% of Australian respondents are from privately owned companies. Of those, 10% of respondents are from family run companies, 38% of respondents are from companies backed by private equity, 26% of respondents are from partnerships and 14% of respondents are from owner-managed companies. With the remaining 12% consisting of publicly listed companies (11% of respondents) and G&PS (1% of respondents).

## Contact us



**Corinne Best**  
Trust and Risk Business Leader  
+61 421 614 344  
corinne.best@pwc.com



**Robert Di Pietro**  
Cybersecurity & Digital Trust Leader  
+61 418 533 346  
robert.di.pietro@pwc.com



**Mike Cerny**  
Partner, Cybersecurity & Digital Trust  
+61 412 414 853  
michael.cerny@pwc.com



**Ryan Menezes**  
Partner, Cybersecurity & Digital Trust  
+61 423 761 085  
ryan.menezes@pwc.com



**Anne-Louise Brown,**  
Senior Manager,  
Cybersecurity & Digital Trust  
+61 406 987 050  
anne-louise.brown@pwc.com

## Explore more

[pwc.com.au](http://pwc.com.au)

© 2022 PricewaterhouseCoopers. All rights reserved. PwC refers to the Australia member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see [www.pwc.com/structure](http://www.pwc.com/structure) for further details. This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors. Liability limited by a scheme approved under Professional Standards Legislation.

At PwC Australia our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 276,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at [www.pwc.com.au](http://www.pwc.com.au)

D0380260