Commvault

The State of Data Resilience

Australia & New Zealand
6th Edition

February 2026

A Tech Research Asia Insights Report (now part of Omdia), commissioned by Commvault

Omdia by informa techtarget

Introduction

This 6th edition of this report series focuses on how organisations across Australia and New Zealand (ANZ) are approaching the issues of cyber resiliency and what impact artificial intelligence is having in this context.

We have continued to focus on key aspects from previous editions that readers identified as important (including trends in data infrastructure, gap between business expectations of breach recovery and the technological reality) alongside research and analysis into the following areas:

- **The most important trends shaping cyber resiliency strategy in an era of both regulatory change and growth in artificial intelligence (AI).**
- **Tracking data growth trends, the infrastructure to support these, and the top challenges in a multi-infrastructure environment that undermine cyber resiliency efforts.**
- **The implications of AI deployments on trust, transparency, and resiliency, as well as identifying the key requirements organisations need from AI solutions to support cyber resiliency needs.**
- **How differences in adoption of identity management strategies for human and non-human (e.g. Agentic AI) impact cyber resiliency and the common hurdles businesses face with identity management and agentic AI.**
- **The disconnect between business expectations on time to recover after a breach and the actual time needed, and why this places pressure on paying ransomware demands from threat actors.**
- **Why defining the necessary components of a minimum viable company (MVC) when under attack is more effective than paying a ransom demand.**

We close our research with an overview of how partner skills are evolving as organisations move from recovery to resiliency.

We hope that you find value in comparing your organisation to your ANZ peers and the report helps you to enhance and strengthen your own data management, recovery, and cyber resiliency capabilities.

If you're curious about the experience of organisations in greater Asia, look for our sister report **The State of Data Resilience, Asia, 3rd edition, 2026.**

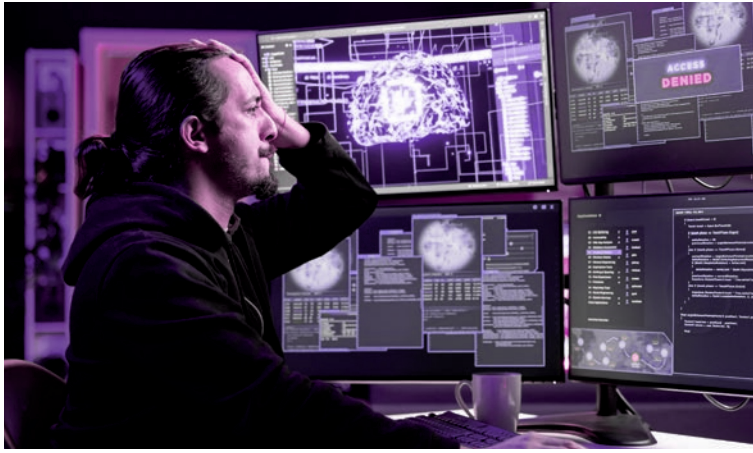
If You Only Read One Page, Read This

Organisations are moving from a defend-and-block cybersecurity strategy to a get-hit-and-keep-going cyber resiliency one. Regulations are slowly moving organisations towards a minimum viable company approach whilst the weaponisation of AI by threat actors increasingly suggest that a breach is inevitable.

AI, especially agentic, can be both a blessing and a curse. The data shows both adoption intent and budgeted AI spend is slated to increase throughout 2026. Agentic AI tools are finding their way into cybersecurity, IT and business operations yet organisations do not always undertake stringent due diligence on the risks these tools bring before deploying them. Nor do they fully trust knowing if the tools are compromised, underperforming, or breaching governance and compliance requirements.

There is a discrepancy between the time that line of business executives expect to be back in operation, and the actual reality of recovery. The data shows that over time, business expectations for a speedy return to a minimal level of operation have increased, whilst tolerance for extended outages (more than 5 days) has fallen.

This recovery expectation imposes even more pressure on organisations while they are subject to a breach. The expectation of 'keeping the lights on', and the complexity of recovery environments for many organisations, means it is inevitable that some organisations simply look to pay the ransom and return to work: a high-risk strategy that typically backfires when the threat actor either refuses to release the data or realises it and attacks again, demanding another ransom.



Top 5 factors impacting cyber resiliency

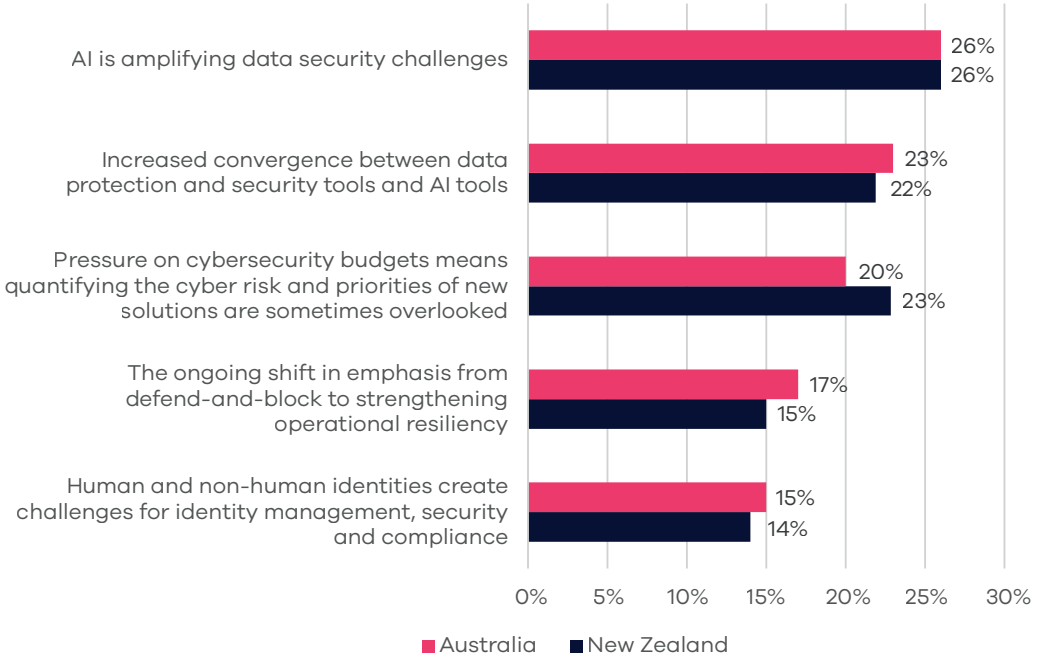
Across Australia and New Zealand (ANZ), cyber resiliency is establishing itself as a board and executive-level priority for organisations. Shifts in cybersecurity strategy, addressing AI and budget considerations are critical influences.

Driven by year-on-year growth in data estates, expanding regulatory requirements, and sustained high levels of ransomware activity, our research reveals the top 5 most important cyber resiliency issues companies are grappling with:

1. The amplification of data security challenges by artificial intelligence (AI) amongst other problems including the speed and scale of attacks, adaptive malware, and exploiting business AI environments.
2. Increasing convergence between data protection and security tools and AI tools means organisations can benefit as reactive, manual processes move towards an automated, predictive, and intelligent state… if they're ready for it.
3. Cybersecurity budget considerations means quantifying cyber risk and priorities is even more critical, however the speed of change and deployment of AI solutions sometimes compromises due diligence prior to deployment.
4. The shift from defend-and-block to establishing a minimum viable company is triggering a change in established cybersecurity operations
5. As agentic AI solutions become more common risk, identity management environments will need to evolve to more effectively address non-human data access, security, and governance requirements.

What are the top 5 trends impacting your cyber resiliency capabilities?

Australia and New Zealand, 2026



Data infrastructure & growth

Data growth rates have re-accelerated. As with previous years, multi-infrastructure environments are the default location.

Unlike the previous two years which saw a decline in ANZ data growth rates, the latest data shows an acceleration of growth at 31% in the 12 months to January 2026, a 4% increase on 2025.

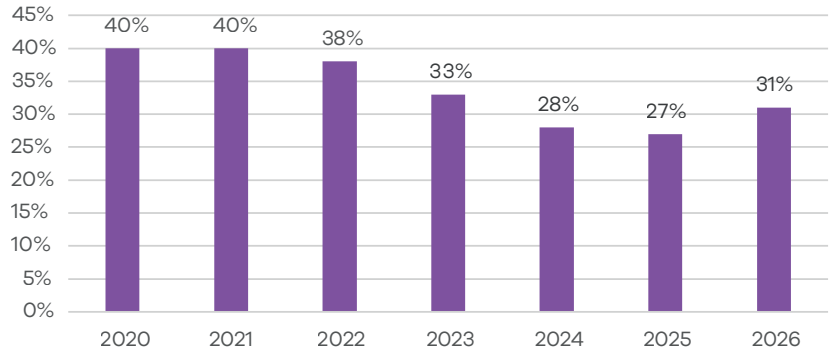
This increase reflects factors including AI-driven data creation, richer telemetry, expanding regulatory retention requirements, and ongoing digital transformation programmes.

This growth is re-establishing upward pressure on storage, protection, compliance complexity, and costs, particularly in areas where dark data is present and consequent data lifecycle management is immature. Incorrectly handled agentic AI can exacerbate these issues (more on this later in the report).

As our previous ANZ research has shown, a multi-infrastructure environment for data and workloads has been the favoured approach for the majority of organisations since 2020. This year is no different with multi-infrastructure (multi-cloud and hybrid) dominant in 67% of ANZ organisations surveyed.

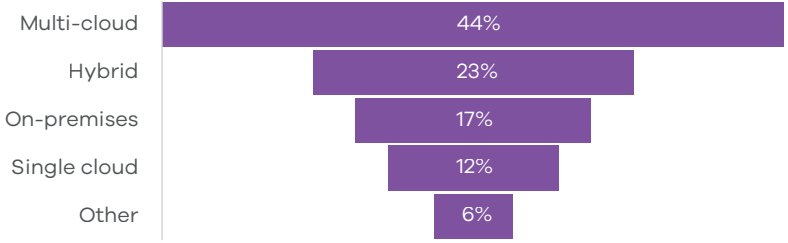
From recovery and cyber resiliency perspectives, our research revealed several multi-infrastructure common obstacles for organisations to overcome.

Average Annual Data Growth Rate in ANZ 2020 - 2026



Which best describes the infrastructure on which your data resides?

Australia and New Zealand, 2026



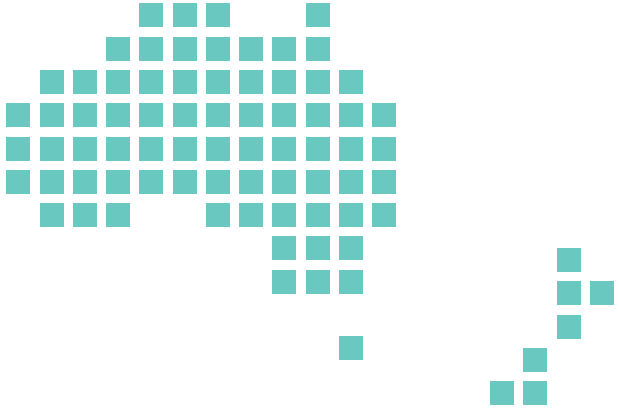
Top 5 multi-infrastructure issues undermining resiliency

A multi-infrastructure data strategy brings benefits, as long as common obstacles are recognised and addressed.

The multi-infrastructure approach reflects a 'best-fit' location for workloads, localisation requirements, and requirements for data to reside in different clouds (in some instances).

As data estates grow through more unstructured data and AI generated content, the fragmentation of tools and skill sets across both cloud and physical infrastructure alongside this also increases the difficulty organisations will experience in maintaining consistent security controls, visibility, and recovery capabilities.

We asked organisations to identify the most significant obstacles faced in across cybersecurity, resiliency, and data management operations. The top 5 are listed on the following page.



Australia

Cybersecurity	Cyber Resiliency	Data Management
Cross cloud solution incident response teams have disparate skills sets **(48%)**	Our ability to recover after an attack or breach is too slow **(35%)**	Reduced efficiency resulting from poor storage and data lifecycle management **(39%)**
Our ability to recover after an attack or breach is too slow **(33%)**	Difficulty confirming integrity and cleanliness of backups **(27%)**	Difficulty confirming integrity and cleanliness of backups **(35%)**
Our threat detection performance is not quick enough **(33%)**	Disparate tools or processes across different environments **(27%)**	Disparate tools or processes across different environments **(33%)**
Difficulty confirming integrity and cleanliness of backups **(32%)**	Lack of current recovery playbooks adaptable for hybrid attacks **(24%)**	Our ability to recover after an attack or breach is too slow **(31%)**
Lack of current recovery playbooks adaptable for hybrid attacks **(26%)**	Our threat detection performance is not quick enough **(22%)**	Our threat detection performance is not quick enough **(29%)**

New Zealand

Cybersecurity	Cyber Resiliency	Data Management
Cross cloud solution incident response teams have disparate skills sets **(42%)**	Our ability to recover after an attack or breach is too slow **(37%)**	Our ability to recover after an attack or breach is too slow **(39%)**
Lack of current recovery playbooks adaptable for hybrid attacks **(32%)**	Disparate tools or processes across different environments **(35%)**	Reduced efficiency resulting from poor storage and data lifecycle management **(38%)**
Our threat detection performance is not quick enough **(31%)**	Our threat detection performance is not quick enough **(27%)**	Difficulty confirming integrity and cleanliness of backups **(36%)**
Disparate tools or processes across different environments **(28%)**	Lack of current recovery playbooks adaptable for hybrid attacks **(24%)**	Our threat detection performance is not quick enough **(32%)**
Incomplete or out-of-date inventory of data and critical systems **(28%)**	Difficulty confirming integrity and cleanliness of backups **(23%)**	Disparate tools or processes across different environments **(30%)**

AI spending intent and agentic AI adoption

AI intent is clear, budgets are increasing, and companies are making progress around policies to protect AI-generated content.

As mentioned earlier, AI is contributing to data growth and is also seen as a tool to support resiliency and cybersecurity activities.

More data created, more complex data infrastructures to manage, and more dollars to be invested. In fact, AI investment is expected to increase throughout 2026, with 95% of companies increasing budgets, 36% of which are raising spend by more than 25% (from 2025).*

Agentic AI (autonomous agents) are attracting a considerable share of overall AI budgets. The data shows that agentic AI is being used across multiple aspects of business operations, including IT, cybersecurity and business processes.

Across these three areas in both Australia and New Zealand, trials or deployments of agentic AI are occurring in more than 30% of organisations.

As data estates grow and AI usage increases, it is important that AI-generated artefacts are governed with the same rigour as traditional data assets.

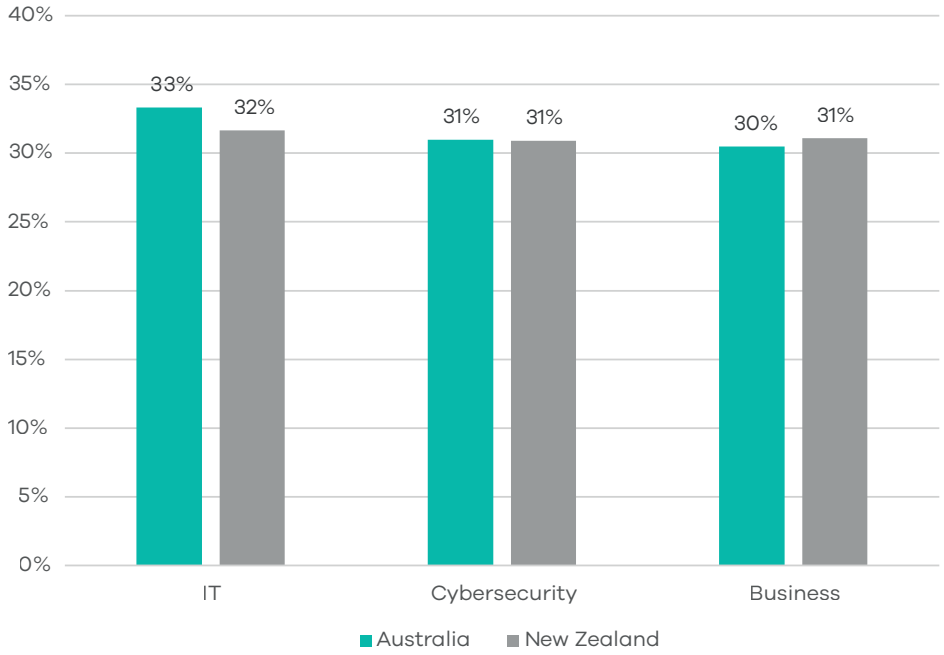
Pleasingly, our data shows progress: in 2026, 66% of companies have governance, risk and compliance (GRC) policies in place to protect AI-generated data and content, a significant increase over 2025's 29%.

However, our data also reveals 2 critical issues influencing the success of organisations' resiliency capabilities.

**Source: Omdia AI Market Maturity September 2025*

Are you trialling or have deployed agentic AI across these areas of your organisation?

Australia and New Zealand, 2026



Organisations lack trust in their AI tools

If deploying AI early and quickly for competitive advantage, make sure you don't skimp on the due diligence.

The 2 flaws we mentioned on the previous page? **Speed to deploy** and a **lack of trust and transparency** in AI processes.

Some organisations are rushing AI tools into deployment without necessary due diligence.

In our 2025 report we noted that "Currently, the allure of AI benefits outweigh the potential cybersecurity risks and concerns."

This year, when asked whether they had undertaken a thorough audit and review of the security and GRC implications of AI solutions before deployment, only 36% of Australian companies and 28% of New Zealand ones indicated they had conducted a 'thorough' assessment.

There is clearly a desire to move quickly to gain maximum competitive advantage through deploying AI.

However, even when deployed, less than 50% of companies in Australia and New Zealand are 'very confident' they are getting the right outcomes from their AI tools. This lack of trust is multi factor too, spanning mistakes, compromised tools, GRC breaches, and data guardrails.

With this in mind, let's take a deeper look into cybersecurity, resiliency, and the use of AI.

How confident are you that your business can identify the following AI errors?

"Very confidently" identify	Australia	New Zealand
Made a mistake	48%	41%
Been compromised	39%	48%
Broken GRC requirements	47%	37%
Compromised data access guardrails	44%	39%

Cybersecurity, resiliency and the use of AI

There is no question AI is changing the cybersecurity landscape as well as how organisations build resiliency capabilities.

Despite some of the concerns raised on the previous page, research data shows that less than 10% of organisations in Asia Pacific have no plans to use AI*.

If anything, our data confirms AI's rapid shift from experimental capability to a core component of modern-day security strategies and architectures.

For those that are adopting and deploying, the drivers are very clear: boost productivity, decrease costs, quicken and scale automation, and reduce risk and cybersecurity exposure.

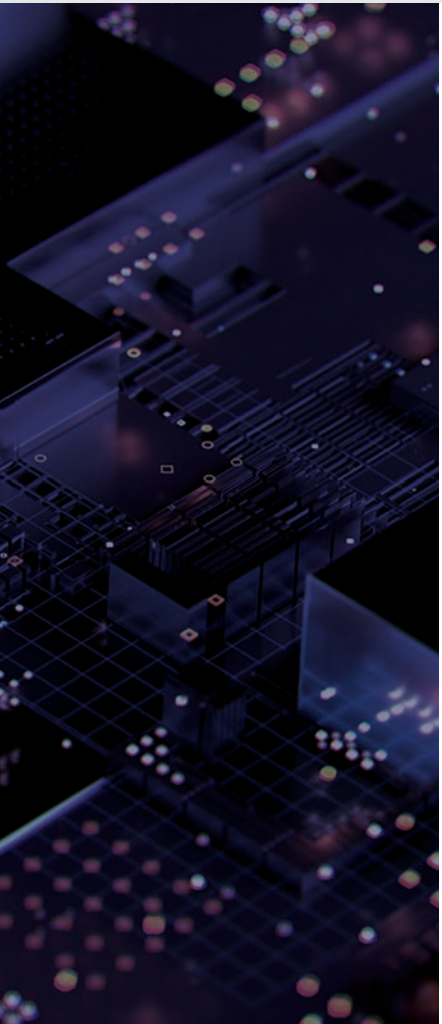
So, what are the most common use cases for AI-augmented cybersecurity solutions?

There is close commonality amongst the use cases for companies in both Australia and New Zealand with improving processes, automation, detection and protection.

New Zealand firms also show a higher focus on reducing workload and fatigue, both key contributors to cybersecurity burnout (and consequent increased risk of breaches).

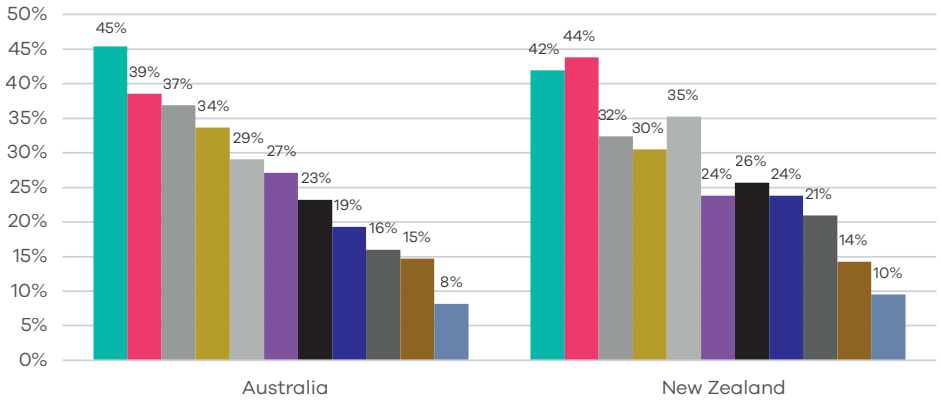
With organisations clearly focusing on improving their resiliency capabilities through AI, what are the main solution attributes they're looking for from vendors?

Source: Omdia AI Market Maturity September 2025



AI Cybersecurity Deployment Use Case

Australia and New Zealand, 2026



- Improving threat detection speed and accuracy
- Automating incident response and remediation
- Enhancing behavioural analytics and anomaly detection
- Strengthening data privacy and protection measures
- Reducing manual workload and alert fatigue in the Security Operations Centre
- Proactively identifying novel threats (zero-day, AI-driven attacks)
- Improving patch and vulnerability management
- Monitoring supply chain, third-party, or cloud security risks
- Responding to AI-powered ransomware and phishing campaigns
- Upgrading legacy security infrastructure for AI compatibility
- None, we are not considering

AI for Cyber: Solution requirements

Move fast, but don't break things. Speed, trust, and compliance are the top considerations for companies looking to boost their resiliency capabilities with AI tools.

Reflecting concerns around trust from earlier on in this report, the most valued attributes are explainability and auditability. These in turn support security, risk and compliance teams in understanding, justifying, and reviewing AI-driven decisions and actions.

Integration into existing tools and workflows, quick and accurate threat detection, and robust automation and orchestration of incident response are all important to ensure AI augments security and resiliency operations.

For Australian organisations the key requirements are:

1. Accuracy and speed of threat detection
2. Explainability and transparency of AI decisions
3. Compliance with regulatory and reporting requirements

For New Zealand, they are:

1. Explainability and transparency of AI decisions
2. Compliance with regulatory and reporting requirements
3. Accuracy and speed of threat detection

One issue that our research surfaced concerns the implications for agentic AI on organisations' identity management capabilities and we delve more into this in the coming commentary.

What are the key solution attributes to support cyber resiliency?

Australia and New Zealand, 2026

Human and non-human agents

There is a clear lag with organisations' cyber resiliency planning and capabilities incorporating non-human agents.

66% of Australian firms and 68% of those in New Zealand incorporate managing human identities in their cyber resiliency plans. That's a solid start.

Unfortunately, by comparison, the inclusion of non-human agents is much lower, standing at 36% and 26% respectively.

Even for organisations currently not using their own agents, many of their suppliers and customers will be. Building agent policies and strategies into cyber resiliency plans is critical.

A number factors explain this lag, including:

Cyber resiliency frameworks have historically focused on human risk, with established playbooks for phishing, insider threats, training, role-based access, etc. tied to people. Equivalent standardised approaches for AI agents are less mature.

Human users are visible, regulated, and auditable, making them a central focus for governance, compliance, and board reporting. By comparison, non-human agentic AI identities are often poorly inventoried, loosely owned, and sometimes treated as shadow IT.

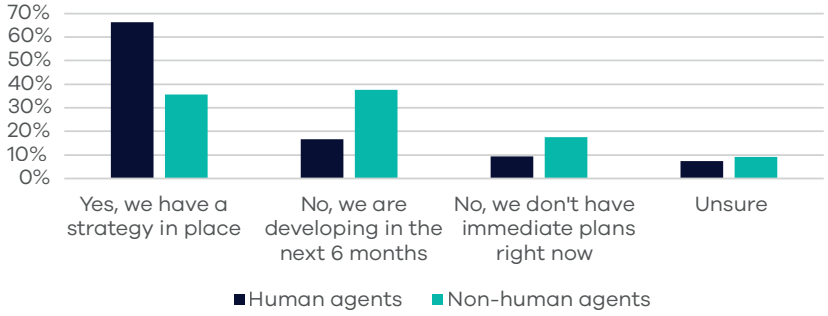
Budget, skills, and processes in cyber resilience are still oriented toward awareness programs, behavioural change, and human control, leaving fewer dedicated resources and metrics to design, test, and rehearse specific to autonomous AI agents.

Agentic AI introduces fast-evolving, potentially poorly understood risks (ephemeral identities, over-permissioned agents, prompt injection, agent-to-agent escalation), and many organisations are still in experimentation mode.

For those considering using agentic AI, our research revealed several key challenges to consider on the next page.

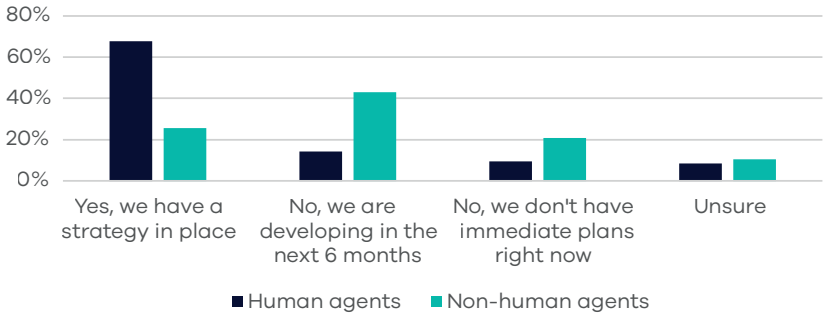
AUSTRALIA

Does your cyber resiliency plan incorporate managing identities for both human and non-human agents?



NEW ZEALAND

Does your cyber resiliency plan incorporate managing identities for both human and non-human agents?



Agentic AI and identity management challenges

Agentic AI. A blessing and a curse.

As we noted earlier, organisations in Australia and New Zealand are deploying or trialling agentic AI across multiple areas – cybersecurity, IT and business operations.

These agents touch multiple areas of the business – customers, partners, suppliers, employees – in many instances elevating the company's risk profile around customers, cybersecurity and recovery (amongst others).

Our data shows organisations are aware that agents bring additional complications: 70% of Australian firms and 73% of those in New Zealand state that agentic AI has a medium or high impact on increased complications around both identity management as well as resiliency operations.

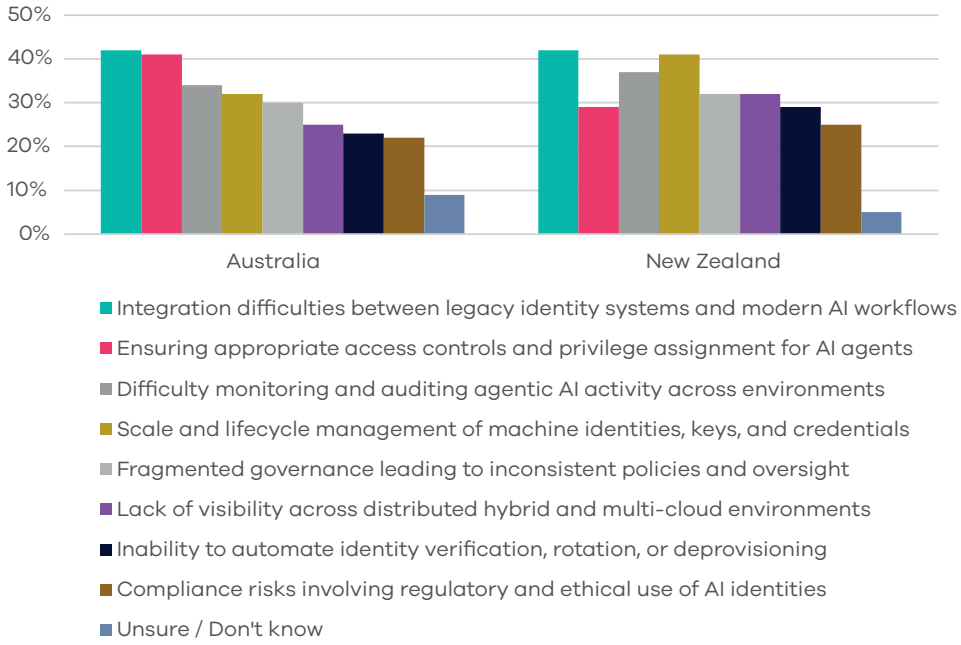
What are these complications?

Difficulties in integration between legacy human-focused identity management systems and those running AI workflows. The sheer scale of, and interconnection with other, machine identities can strain capabilities and agent life-cycle management.

Access and privilege for non-human agents places greater demands on systems due to the dynamic and ephemeral nature of agents being spun up and down.

Once again, confidence and trust in AI tools performing as they should is low. This compounds when it is generally difficult to monitor agentic activity across different environments.

Top challenges with managing non-human identities of agentic AI
Australia and New Zealand, 2026



Breach recovery expectations and reality

Business executives want to be back in business within 5 days. The reality is somewhat different.

More data, more locations, more workloads and more regulations. Things get tough when an organisation is breached.

As previous editions of this report have surfaced, there is still a considerable disconnect between the time senior business executives expect to be back in business and the reality of recovery in a complex technology environment.

This disconnect continues today.

For business leaders, speed of resuming business operations is the critical factor – 30% of Australian leaders and 35% of those in New Zealand expect to be 'back in business' in 1 day.

After 5 days, those numbers increase to 82% and 84% respectively.

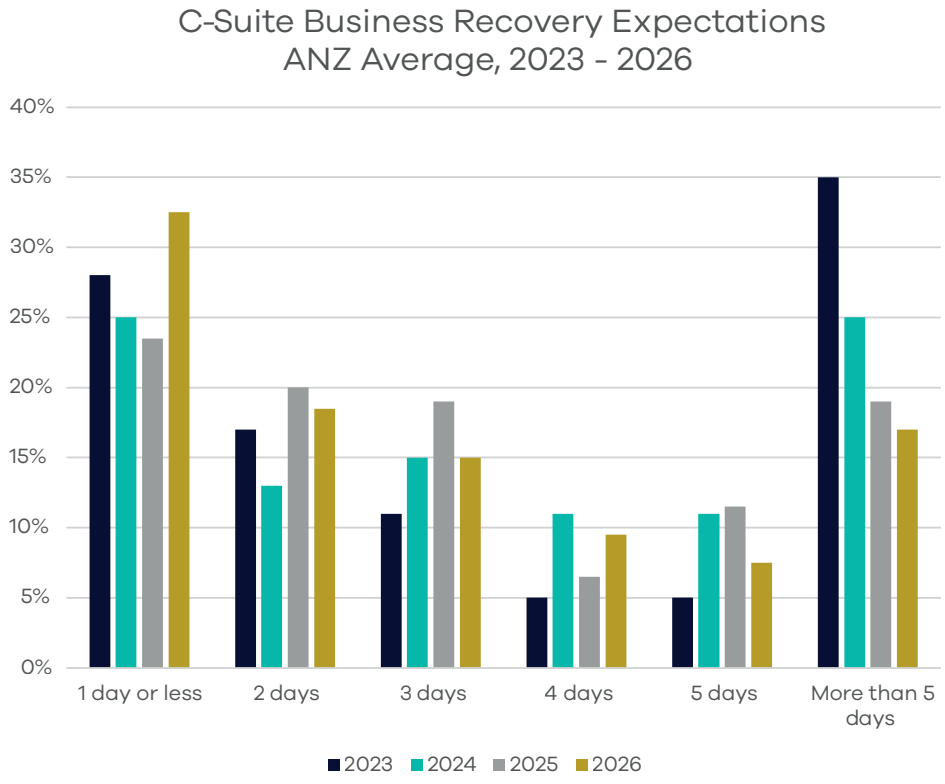
The reality? On average, time to recover to a minimal level of operation is 28 days for both Australia and New Zealand.

The data shows that over time, business expectations regarding a speedy return to a minimal level of operations have increased, whilst tolerance for extended outages (more than 5 days) has dropped.

The silver lining? Despite increased complexities, on average, the time to recover to a minimal operational level has fallen from 42 days in 2023 to 28 days in 2026.

If breaches are ultimately inevitable, how can you ensure the smallest possible disruption to your business, customers, suppliers, and employees in the shortest time available?

Is it better to simply pay the ransom and move on?


C-Suite Business Recovery Expectations
ANZ Average, 2023 - 2026
40%
35%
30%
25%
20%
15%
10%
5%
0%
1 day or less
2 days
3 days
4 days
5 days
More than 5 days
2023
2024
2025
2026

Ransomware payment effectiveness

Pay the ransom? Sure, roll the dice and hope criminals are feeling 'generous'

Is it easier and quicker to pay?

No, the data shows that the majority choose not to pay, and for those that do, there is no guarantee that data access will be restored.

Amount of companies that have been targetedAn average of 44% of companies in ANZ and Asia surveyed report being targeted with ransomware in the last 12 months.

Which factors do they consider when deciding to pay? Considerations range from the speed of recovery, to cost and risk implications. The top 5 factors influencing ANZ organisations are revealed in the table to the right.

Do they pay?

Whilst the policy may be to not pay, once breached some companies do buckle under operational and time pressures.

30% of Australian organisations and 34% in New Zealand stated they paid the demand.

Does it work?

Not really. Of those in Australia and New Zealand that paid ransoms, respectively 46% and 36% stated it didn't work as the threat actor did not release the data, or if they did, quickly attacked again, demanding additional payment.

Considerations when deciding to pay a ransom

Australia	New Zealand
Confidence in the integrity and completeness of backups	Reputational and legal risks associated with payment
Reputational and legal risks associated with payment	The ransomware cost
Expected speed of non-payment recovery compared with paying the ransom	Confidence in the integrity and completeness of backups
The ransomware cost	Advice from legal, regulatory, or cyber insurance brokers
Advice from legal, regulatory, or cyber insurance brokers	Expected speed of non-payment recovery compared with paying the ransom

The importance of defining your Minimum Viable Company (MVC)

Having a defined MVC strategy for both business and technology operations significantly boosts the chance of keeping the lights on when attacked.

Broadly speaking, MVC planning needs to incorporate technology, cultural, and business considerations starting with the question of 'what is the bare minimum my business requires to ensure it can continue to operate and serve customers?'.

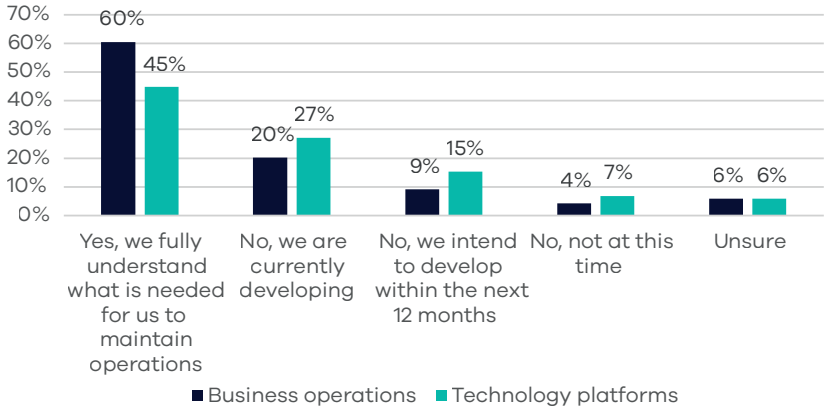
Our data shows that clearly identifying minimum technology requirements to ensure a base level of business operations during an attack significantly improves the chance of recovery.

Australian and New Zealand organisations with defined minimum levels of operational business requirements linked to clear technology capabilities are 3.5 and 1.8 times respectively more likely to maintain operations when attacked and recover faster, than those with an undefined level.

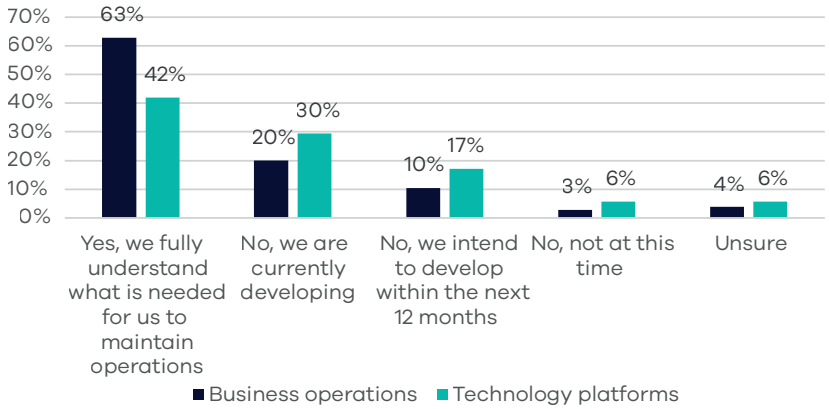
- 60% of Australian and 63% of New Zealand organisations have defined MVC requirements for their business operations.
- By comparison, 45% of Australian and 42% of New Zealand organisations have defined MVC requirements for their technology environments.

There is much to consider and unsurprisingly, many organisations look to technology partners to help build and support cyber resiliency capabilities. As companies move from traditional backup and recovery operations to cyber resiliency, partner skills and competencies also change, as we outline on the next page.

AUSTRALIA



NEW ZEALAND



Partner skills matrix

Early in our report we noted the move from defend-and-block to establishing a minimum viable company capacity. For many organisations, they are now looking to partners that can offer a holistic skill set spanning multiple areas including data infrastructure management, cyber resiliency capabilities, AI skills and knowledge, and proficiency in identity management across both human and non-human agents. Here are the top 5 skills that customers need from their partners across each of these areas.

Australia

Data Infrastructure	Cyber Resiliency	Artificial Intelligence	Identity Access Management
Monitoring, incident detection and rapid problem resolution	Backup and data protection management	Advanced AI model development and integration skills	Real-time suspicious identity activity monitoring
Advanced cybersecurity expertise for threat prevention & compliance	Digital forensics and breach investigation	Expertise with all data formats – structured, unstructured, media, etc.	Strong governance and compliance frameworks
Ability to integrate, automate and optimise legacy and new infrastructures	Ransomware remediation and negotiation support	Data management, access, regulatory and compliance skills	Advanced automated pro/ deprovision and access control
Technical cloud, network and platform management skills	Incident response expertise	AI explainability, documentation and reporting skills	Expert multi-infrastructure identity management
Strategic planning for scalability, transformation & cost management	Cloud migration and architecture design	Data privacy, security and risk management control skills	Human/non-human integration AI systems and workflows

New Zealand

Data Infrastructure	Cyber Resiliency	Artificial Intelligence	Identity Access Management
Monitoring, incident detection and rapid problem resolution	Backup and data protection management	Expertise with all data formats – structured, unstructured, media, etc.	Real-time suspicious identity activity monitoring
Advanced cybersecurity expertise for threat prevention & compliance	Digital forensics and breach investigation	Advanced AI model development and integration skills	Expert multi-infrastructure identity management
Strategic planning for scalability, transformation & cost management	MDR and SOC expertise	AI explainability, documentation and reporting skills	Advanced automated pro/ deprovision and access control
Technical cloud, network and platform management skills	Regulatory compliance and audit readiness skills	Data management, access, regulatory and compliance skills	Human/non-human integration AI systems and workflows
Ability to integrate, automate and optimise legacy and new infrastructures	Ransomware remediation and negotiation support	Proven customer success and experience	Strong governance and compliance frameworks

In Closing

The transition from defend-and-block to get-hit-and-keep-going represents a significant change in how organisations across Australia and New Zealand approach cyber resilience.

Regulations focusing on resiliency, accelerating data growth, the weaponisation of AI, and the complexity of managing security across multi-infrastructure environments means organisations must move beyond reactive incident response and invest strategically in defining their minimum viable company (MVC).

Yes, paying the ransom might work. Once, but again, and again, and again? As the disconnect between the business expectations of rapid recovery and the operational reality pressures organisations toward the false economy of ransom payments, the importance of an established MVC strategy becomes even more paramount.

Commvault Perspective

The findings in this report reinforce a reality Commvault sees every day across the region: resilience is no longer a static capability or a point solution – it is an operating model. As organisations in Australia and New Zealand accelerate AI adoption, expand data estates, and operate across increasingly complex hybrid and multi-cloud environments, resilience must be engineered into day-to-day operations, not bolted on after an incident.

This research highlights three areas where organisations must rethink how they prepare for and operate during disruption.

Minimum viability is now the foundation of cyber resilience

The shift towards a minimum viable company (MVC) mindset represents a fundamental change in how organisations approach cyber risk. The data shows that breaches are no longer an outlier event; they are an operational certainty. In this context, resilience is defined by how quickly and confidently an organisation can restore what matters most, not everything.

We see progressive organisations are the ones moving beyond traditional backup and recovery toward a cyber resilience platform approach that identifies, protects, and rapidly recovers the data, applications, and identities that underpin minimum viable operations. Organisations that clearly define MVC – and those linking business priorities to recoverable technology capabilities – are far better positioned to keep the lights on, avoid ransom-driven decisions, and maintain trust with customers, regulators, and partners.

Closing the gap between business expectations and recovery reality requires a new operating model

This report again exposes a persistent disconnect: executives expect to be operational within days, while recovery in real-world environments still takes weeks. As data volumes grow, infrastructures fragment, and regulatory pressure increases. This gap becomes more dangerous – not just costly.

Closing it requires more than better tools. It requires ResOps: a resilience-first operating model that treats recovery, cyber response, and data protection as continuous, integrated functions. In a ResOps model, organisations unify security, IT operations, and data management around common visibility, automation,

and recovery objectives. Clean data recovery, verified backups, rehearsed recovery playbooks, and AI-assisted orchestration are no longer emergency measures – they are standard operating practice.

Commvault sees ResOps as the natural evolution of SecOps and DevOps: an always-on discipline focused on operational survivability, not just incident response.

AI resilience and due diligence are critical to sustaining trust and value

AI is rapidly becoming embedded across business operations, IT, and cybersecurity. This research confirms both its promise and its risk. While AI can dramatically improve threat detection, recovery speed, and operational efficiency, rushing deployment without due diligence undermines resilience and trust.

From Commvault's perspective, AI resilience means ensuring AI systems, AI-generated data, and AI agents are protected, governed, and recoverable by design. Explainability, auditability, and compliance are prerequisites for safe adoption, not optional features. This is especially true as agentic AI introduces large numbers of non-human identities that operate autonomously across environments.

Resilient organisations apply consistent data and identity management principles across both human and machine actors, ensuring that AI augments cyber resilience without compromise. AI should strengthen ResOps by accelerating detection, validating recovery integrity, and automating response, while remaining transparent, controlled, and trustworthy.

In summary, this edition's research reinforces that readiness for the AI era is inseparable from resilience. Organisations that define minimum viability, operationalise recovery through ResOps, and adopt AI with discipline will be better equipped to withstand disruption and continue moving forward.

Commvault's cyber resilience platform is purpose-built to support this shift, bringing together data security, rapid recovery, identity awareness, and AI-driven automation at enterprise scale. This allows organisations to move from simply reacting to incidents to operating with confidence, even in the face of inevitable disruption.

Key Country Data Points: Australia

This page summarises key data points from the commissioned survey.

Data growth in 12 months to 2026: 30%

Data infrastructure (now and last year):

- Hybrid: 23% (24%)
- Multi-cloud: 40% (36%)
- On-premises: 17% (21%)
- Single cloud: 13% (13%)
- Other: 7% (6%)

Top 3 AI cybersecurity use cases

1. Improving threat detection speed and accuracy
2. Automating incident response and remediation
3. Enhancing behavioural analytics and anomaly detection

Top 3 AI cybersecurity solution requirements

1. Accuracy and speed of threat detection
2. Explainability and transparency of AI decisions
3. Compliance with regulatory and reporting requirements

How confident are you that your business can identify the following AI errors? 'Very high'

- Make a mistake: 48%
- Been compromised: 39%
- Broken GRC requirements: 47%
- Compromised data access guardrails: 44%

Has your organisation undertaken a thorough audit of security and GRC implications of AI solutions before they were deployed? 'Yes': 38%

Deployment of agentic AI (% trialling or adopted)

- IT operations: 33%
- Cybersecurity operations: 31%
- Business operations: 30%

Top 3 agentic AI challenges:

1. Integration difficulties between legacy systems and modern AI workflows
2. Ensuring appropriate access controls and privilege assignments for AI agents
3. Difficulty monitoring and auditing agentic AI activity across environments

Incorporating human and non-human agent identity management into cyber resiliency plans. 'Yes, we have a strategy'

- Human: 66%
- Non-human: 36%

Have you been targeted by a ransomware attack? 'Yes': 30%

Top 3 ransomware payment considerations:

- Confidence in the integrity and completeness of backups
- Reputation and legal risks associated with payment
- Expected speed of non-payment recovery compared with paying the ransom

Pay or not pay? 30% paid

Payment success? 'No': 46%

Defined MVB in your resiliency strategy and capabilities? 'Yes'

- Business operations: 60%
- Technology operations: 45%

Key Country Data Points: New Zealand

This page summarises key data points from the commissioned survey.

Data growth in 12 months to 2026: 30%

Data infrastructure (now and last year):

- Hybrid: 22% (24%)
- Multi-cloud: 47% (39%)
- On-premises: 16% (18%)
- Single cloud: 11% (11%)
- Other: 4% (8%)

Top 3 AI cybersecurity use cases

1. Automating incident response and remediation
2. Improving threat detection speed and accuracy
3. Reducing manual workload and alert fatigue in security operations centre

Top 3 AI cybersecurity solution requirements

1. Explainability and transparency of AI decisions
2. Compliance with regulatory and reporting requirements
3. Accuracy and speed of threat detection

How confident are you that your business can identify the following AI errors? 'Very high'

- Make a mistake: 41%
- Been compromised: 48%
- Broken GRC requirements: 37%
- Compromised data access guardrails: 39%

Has your organisation undertaken a thorough audit of security and GRC implications of AI solutions before they were deployed? 'Yes': 38%

Deployment of agentic AI (% trialling or adopted)

- IT operations: 33%
- Cybersecurity operations: 31%
- Business operations: 31%

Top 3 agentic AI challenges:

1. Integration difficulties between legacy identity systems and modern AI workflows
2. Scale and lifecycle management of machine identities, keys and credentials
3. Difficulty monitoring and auditing agentic AI activity across environments

Incorporating human and non-human agent identity management into cyber resiliency plans. 'Yes, we have a strategy'

- Human: 66%
- Non-human: 36%

Have you been targeted by a ransomware attack? 'Yes': 32%

Top 3 ransomware payment considerations:

- Reputational and legal risks associated with payment
- Cost of the ransom
- Confidence in the integrity and completeness of backups

Pay or not pay? 30% paid

Payment success? 'No': 36%

Defined MVB in your resiliency strategy and capabilities? 'Yes'

- Business operations: 63%
- Technology operations: 42%

Appendix

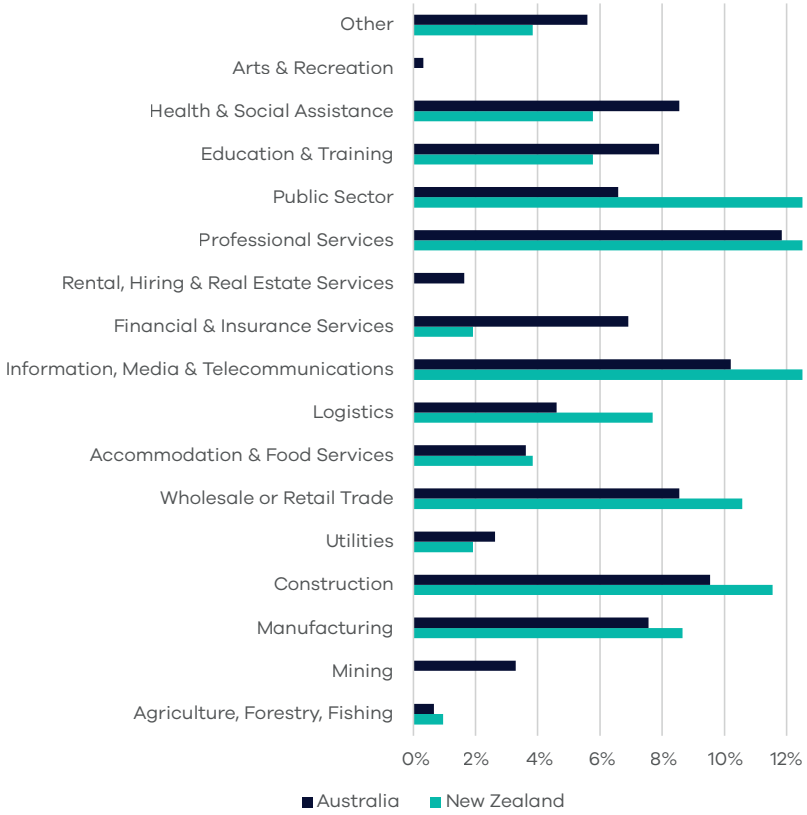
The research methodology and demographics

Using an online panel, TRA (now part of Omdia) conducted an independent quantitative market research survey in December 2025 and January 2026.

The total sample size is 411 organisations (Australia 306 and New Zealand 105) and respondents were CIO/CISO, IT leader, IT decision maker and direct reports.

Australian respondent companies were required to have between 100-199 or 200+ employees, and New Zealand companies 50-199 or 200+ employees. Each country had a 50/50 distribution between employee size groups.

Respondents by Industry



About

Commvault (NASDAQ: CVLT) is the gold standard in cyber resilience, helping more than 100,000 organisations to uncover, take action, and rapidly recover from cyber attacks – keeping data safe and businesses resilient and moving forward. Today, Commvault offers the only cyber resilience platform that combines the best data security and rapid recovery at enterprise scale across any workload, anywhere with advanced AI-driven automation – at the lowest TCO.

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa TechTarget, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

Commvault®

Omdia by informa techtarget