Commvault

THE STATE OF DATA READINESS

CONTINUOUS BUSINESS IN FOCUS

Australia & New Zealand
5th Edition
March 2025

A Tech Research Asia Insights Report,
commissioned by Commvault.

TRA

INTRODUCTION

Welcome to the 5th edition of The State of Data Readiness in ANZ

This edition of provides insights into the data management, cybersecurity, and regulatory challenges faced by organisations in Australia and New Zealand.

In previous report editions, we've consistently focused on:

- **Data – it's year on year growth, the infrastructure on which it resided, and the prevalence of dark data;**
- **The top two issues impeding data management & security;**
- **Business expectations of the time to recover from a cybersecurity breach and how this differed to the recovery reality; and**
- **An overview of cyber attacks, the use of AI in cybersecurity, data recovery rates and breach awareness.**

For this year, we have expanded our research to also include:

- **How changing regulations are impacting organisations' technology strategies;**
- **If companies see a cybersecurity risk when deploying business-focused AI solutions; and**
- **Are companies making progress in strengthening their cybersecurity capabilities – and if so – what is the impact on their ability to maintain operations in the event of an attack or breach.**

We also wanted to see if there were differences in cybersecurity operations and beliefs of companies that experienced a cybersecurity breach and those that have not.

We asked if the experience of being breached changed a company's view of its operations and capabilities, especially in relation to:

- **The deployment and impact of AI-business tools on a company's cybersecurity risk profile;**
- **Effective incident response and recovery operations; and**
- **Expectations for business recovery in light of a breach.**

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 for continuous business.

Sincerely,
Tech Research Asia

**The data provided in this Commvault commissioned TRA Insight Report comes from 408 companies in Australia and New Zealand. Additional information on this sample can be found in the appendix of the report.*

REPORT HIGHLIGHTS

Data growth rates eased in 2024, while the regulatory requirements to which organisations must abide continued to expand. Enthusiasm for AI continues to be strong even in the face of heightened concerns about the impact on an organisation's cyber and risk capabilities. Interdependent sprawl across infrastructure, workloads and data increases the difficulty of both testing incident response plans as well as maintaining minimal viable business operations in the event of an attack or data breach.

The Data Environment:

- Data growth rates have marginally slowed since our previous report, falling from 28% to 27% year on year increases in ANZ.
- 62% of companies operate blended data infrastructure environments (multi-or-hybrid cloud), the same as last year. By 2026, this percentage is expected to rise to 71%.
- 54% of Australian organisations and 63% of New Zealand ones are not confident they understand all the necessary relationships, metadata and configurations required to restore business operations if breached.

The Regulatory Environment:

- 55% of Australian and 53% of New Zealand companies are required to maintain copies of data in different cloud environments to support resiliency capabilities.
- 37% (AU) and 34% (NZ) organisations face conflicting regulatory demands for their data across different geographies.
- 17% are needing to comply with at least four major regulatory acts, 6% are subject to at least 6.

The AI Environment:

- 28% of companies are now subject to AI-related compliance requirements and another 40% expect to be within the coming year.
- 68% of organisations believe adopting business AI solutions increases the likelihood of a cybersecurity breach, yet this has not prevented them deploying AI-business solutions.
- 63% of organisations have not conducted thorough and extensive audits on the security implications of AI tools prior to deploying them.
- 29% have comprehensive policies in place to protect AI-generated data.

The Recovery and Resiliency Environments:

- 12% rate their ability to operate effectively during a cybersecurity incident as 'excellent'. 23% rate themselves as 'bad' or 'terrible' in the same scenario, 65% are middling in their effectiveness.
- 70% have incident response plans (IRPs) in place, 30% test all aspects of their environment as part of IRP activity, 19% only test mission critical workloads.
- Of those breached, 33% lost access to all their data, 74% experienced data exfiltration activity and 1-in-3 (32%) recovered 100% of their data.
- 80% of business leaders expect to recover from a cybersecurity incident within 5 days. 23% want to be back in business within 1 day (or less).
- However, 55% of businesses take more than one-week to recover, with the average being 4 weeks – a significant gap between expectations and reality.
- 70% of ANZ organisations have been subject to a ransomware demand. Of these, 20% stated they have paid.
- Despite 54% of ANZ companies having a 'no payment' ransomware policy, when attacked, 15% of those broke policy and paid anyway.

Considerations

- Australia and New Zealand governments have a history of leading regional developments in privacy, governance and cybersecurity regulations and frameworks. Whilst this is positive for customers, employees and constituents, it does complicate the business operating environment with companies facing complex, sometimes contradictory requirements.
- Changes around AI, business resiliency and cybersecurity regulations will only increase these complications.
- The impact of AI, the complexity of recovering in multi-infrastructure environments, and the disconnect between business expectations and IT reality on responding to attacks and breaches, sees organisations seeking third party support from tech partners to help meet obligations.
- Incident response plans are increasingly under microscopes assessing their efficacy. As the complexity of data environments and regulations increase, organisations must check that the scope, timing and depth of their incident response plans are aligned to maintaining business operations during an attack or breach instead of a reactive, post-incident recovery focus.
- IRPs are important but experiencing a breach is the real test of an organisation's business resiliency. Our data on the next page shows why.

BREACH LESSONS

Does being breached mean better incident response, improved awareness of issues, and a stronger business resiliency stance next time round?

On balance, yes. Mostly.

Our data suggests breached companies have a more pragmatic view of their actual capabilities, the complexities of recovery in multi-infrastructure environments and the reality of what it takes to get back in business including:

- **Clarity on response capability:** Companies not attacked scored themselves 'excellent' in their *'ability to maintain business operations with no disruption'* 2.5 times more than those that had been attacked.
- **Due diligence of AI tools increased post attack:** Those attacked were then 1.5 times more likely to undertake (as part of broader reviews) a thorough and complete review of AI tools and solutions compared to those that had not been attacked.
- **Operational resiliency and back to business:** Companies not attacked were 1.5 times more likely to expect to be back in business within 1 day compared with those that have experienced the reality of an attack.
- **Not being attacked suggests false hope.** Those not attacked rate their expectation of how they would perform if they were attacked as twice as likely to perform well (i.e. clearly understood response plans, communications processes and related IRP activities) compared to the actual performance of those attacked.
- **Comprehensive incident response planning:** Those attacked are twice as likely to test all mission critical workloads and dependencies as part of their IRP compared with those yet to be attacked.

Our data also shows higher cybersecurity maturity levels bring benefits encompassing a number of operational outcomes:

- **Better breach resistance:** Those with very high maturity levels were 5-times more likely to not lose any data compared to those with very low levels.
- **Improved data recovery:** Those with high levels of maturity were almost twice (1.9x) as likely to recover 100% of their data if lost.
- **Lower data lock-out levels:** Relative to those with high maturity, companies with low maturity levels are 4 times more likely to be locked out of their data.
- **Stronger business resiliency:** Companies with high maturity levels were 6-times more likely to maintain business operations during an attack compared to those with low levels.

Let's dive a little more deeply into some of the insights, starting with the trends in data growth and infrastructure.

THE DATA ENVIRONMENT

Data growth rates have eased, and multi-infrastructure environments are the default location for estates. Repatriation from single cloud to on-premises infrastructure has occurred at minimal levels.

Data growth rates remained at similar levels between 2024 and 2025, decreasing 1% from 28% to 27% in that time.

Conversations with organisations in Australia and New Zealand indicate a substantial focus on cleaning and rationalising their data (especially as companies 'tidy' ahead of planned AI initiatives), as well as the continued emphasis on cost reduction, deduplication and storage optimisation that was also present in 2023 and 2024.

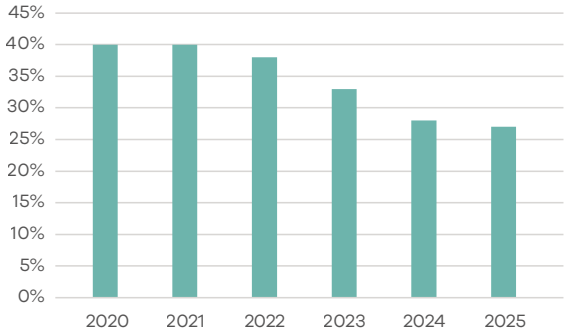
As with 2024, data typically sits in a multi-infrastructure environment for the majority of organisations: 63% of ANZ companies are using a hybrid or multi-cloud approach for their data, unchanged from 2024.

Digging a little deeper also reveals that since 2020, the multi-infrastructure approach has seen little fluctuation, typically sitting around the low-60% range over that time. During the same period, there has been a small drift (low single digit percentages) from single-cloud only infrastructure (typically private cloud) to on-premises environments.

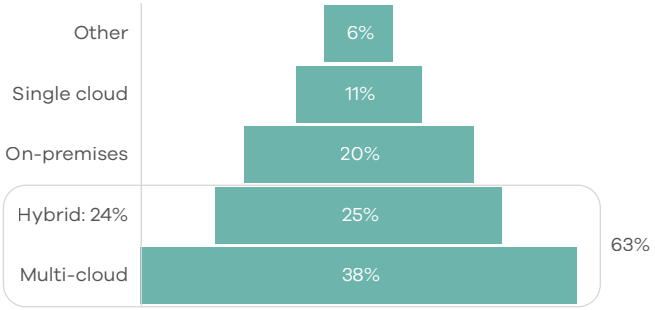
The more significant change is not so much the data or the infrastructure, but rather the changing business resiliency rules and regulations ANZ organisations need to deal with as they go about their day-to-day operations.

We dive into this in more detail in the coming few pages.

Average Annual Data Growth Rate in ANZ
2020 - 2025



"Which best describes the infrastructure on which your data resides?"
ANZ 2025



THE REGULATORY ENVIRONMENT

Changes in data privacy, business resiliency and cybersecurity laws across Australia and New Zealand have significant implications for business' technology environments and capabilities. A non-exhaustive list for each country is outlined here.

Australia

Australia's Privacy Act 1988 has undergone significant strengthening through reforms legislated in late 2024 including:

- Statutory Tort for Invasion of Privacy: A new statutory tort has been introduced for serious, intentional, or reckless invasions of privacy, set to commence in June 20253.
- Transparency for Automated Decision-Making (ADM): New transparency requirements are in place for the use of automated decision-making, with these requirements coming into effect in December 2026.
- Enhanced Powers for the OAIC: The Office of the Australian Information Commissioner (OAIC) has expanded monitoring and investigation powers and can now issue infringement notices for minor violations and compliance notices, indicating a greater focus on enforcement.
- Increased Penalties: New civil and criminal penalties have been introduced, including those associated with doxing.

Cyber Security Legislation: In November 2024, the Australian government passed new cyber security and critical infrastructure legislation including:

- Ransomware Reporting: A ransomware payment reporting framework has been established.
- Risk Management Obligations: New risk management obligations for critical asset owners have been introduced.

Additional Security of Critical Infrastructure (SOCI) Act Amendments including:

- Inclusion of data storage systems holding 'business critical data' within the definition of 'asset.'
- New ministerial powers to direct entities to take specific actions following a critical asset incident.

- New powers for the Home Affairs to direct an entity to address deficiencies in a risk management program.

Specifically for financial services organisations, the Australian Prudential Regulation Authority (APRA) released Prudential Standard CPS 230 Operational Risk Management, taking effect July 1, 2025. This requires APRA-regulated entities to prepare for service disruptions, take action to prevent them, and enhance operational resilience[1].

The implementation of CPS 230 will require substantial alterations in operational risk management, business continuity, key service provider agreements, and governance procedures.

New Zealand

In September 2023, the New Zealand government released the Privacy Amendment Bill (PA Bill), set to come into force on June 1, 2025.

IPP 3A Introduction: A key amendment is the introduction of a new IPP 3A, which requires organisations collecting personal information 'indirectly' to inform individuals about the processing of their data, although some exceptions do exist.

Consumer Data Right: The government expects the Consumer and Product Data Bill will be passed into law in early 2025, establishing a consumer data right in New Zealand

The Privacy Commissioner is empowered to investigate actions that may interfere with individual privacy, either in response to a complaint or on their own initiative. It can also issue compliance notices, requiring agencies to take or cease actions to comply with the Act.

The Financial Markets Authority (FMA) has introduced a new standard condition for certain market license holders, focusing on business continuity and technology systems, which came into effect on July 1, 20244. The new standard condition requires license holders to have and maintain a business continuity plan that is appropriate for the scale and scope of its service.

1 https://www.minterellison.com/articles/cps-230-your-roadmap-to-compliance

THE REGULATORY ENVIRONMENT

Already challenging, getting more complicated, and for some, undermining their ability to either respond quickly to cyber attacks, or recover rapidly post attack.

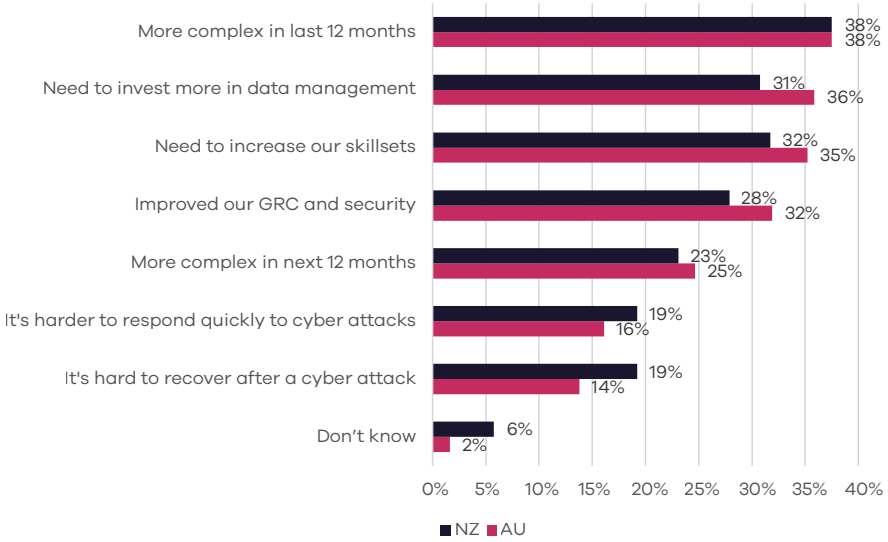
"Regulations make life easy." Said no-one ever. As regulations continue evolving, so too will regulatory challenges and obstacles:

- An average of 62% of ANZ organisations stated that they face (38%), or will face in the coming 12 months (24%), increased complexity and business challenges due to increased regulatory requirements.
- 34% of organisations noted that these laws highlighted a need for additional investment in activities to increase employee GRC and security skillsets.
- 18% reported it's harder to respond quickly to cyber attacks and 17% stated regulations make it hard to recover and restore operations after an attack.
- 54% of organisations state they are already experiencing conflicting regulatory requirements for their data across different geographies.
- 34% of organisations are subject to at least 4 different regulatory and compliance acts (for example, APRA, SOCI, STB, MAS, DORA, GDPR, etc), and another 27% currently 'don't know' what they need to be fully regulatory compliant.
- 54% stated regulations require them to keep copies of their data in either public or private clouds, distinct from their production data.
- As AI adoption has increased, the regulations have moved to incorporate the technology. On average 28% of ANZ companies are now subject to AI specific requirements, with another 40% expected to be so in the coming 12 months.

Pleasingly, 30% acknowledged that the pain is worth the gain stating that responding to the requirements *'improved our GRC and security capabilities'.*

"What has been the impact of the legal and regulatory requirements your organisation must deal with?"

ANZ 2025



THE REGULATORY ENVIRONMENT IMPLICATIONS

Companies face more complex regulatory environments, increased pressure to strengthen cybersecurity and resiliency capabilities, and will need to boost adherence to AI regulations as well.

There's a lot to unbox in the various data privacy and cybersecurity regulations, however three key areas stood out for us:

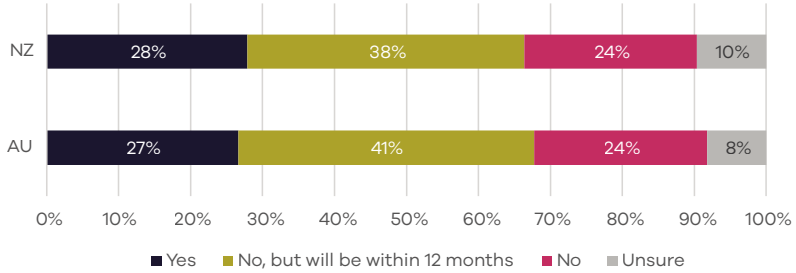
1. **Mandatory data breach notifications:** Many companies must now notify authorities of data breaches with very quick deadlines (in some cases no more than 24-72 hours). Along with establishing Data Protection Offices (DPOs), this means data compliance, management and reporting systems will need to be accurate, rapid and work across multi-infrastructure environments (no easy task).
2. **Cross-border data transfers:** As the data shows in the next page, organisations face multiple, and conflicting, requirements for cross-border data transfers. Data localisation laws also require companies to store certain types of data within sovereign borders.
2. **Operational resiliency:** Regulations are focusing on requiring companies to maintain a minimum level of business operation while subject to data breaches or cybersecurity incidents. It's not just about securing data, it also involves ensuring continuity plans are in place and tested. With blended infrastructure the most common data environment, companies will need both visibility into their data estates as well as deep understanding of the dependencies between meta data, applications, configurations and workloads.

"Does your organisation face regulatory requirements that require you to keep copies of your data in different clouds?"

ANZ 2025

"Is your organisation subject to specific AI regulatory and compliance requirements or legislation?"

ANZ 2025



THE AI ENVIRONMENT

Currently, the allure of AI benefits outweigh the potential cybersecurity risks and concerns. Deployment rates are high despite concerns that deploying business-focused AI solutions increases the risk of a cybersecurity breach or incident. There's work to be done.

73% of ANZ organisations are currently using some form of business-focused AI solution, despite 68% of those believing the usage contributes to increased risk of cybersecurity breach or incidents:

- 15% believe they bring a 'high risk'
- 53% believe they bring 'moderate risk'

With this in mind, and considering 28% of ANZ companies are already subject to some form of regulated usage of AI solutions, are companies really undertaking due diligence and assessing the impact AI has on an organisation's risk posture?

Unfortunately, the high levels of AI hype in the market are making this assessment difficult.

45% of ANZ organisations either 'strongly agree' or 'totally agree' with the statement *"The hype around AI makes it difficult to understand the true risk of using AI tools and solutions in our organisation."*

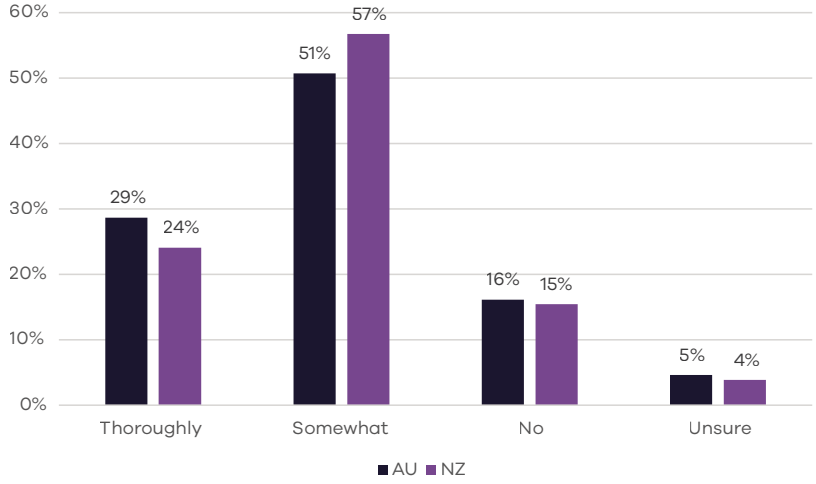
It's understandable. New technology solutions have been oversold on promise since the first 8088 processor PC in the 1970s... still, at least now organisations will be more diligent about vetting solutions before deployment, right?

Well, 27% of them are. Our data shows they undertook a thorough audit and review of the security and governance, risk and compliance implications of AI solutions used in their organisation before deployment.

We also see that 29% have comprehensive policies that are part of a broader cybersecurity and data management strategy to protect data and content created by generative AI solutions.

"Did your organisation undertaken a thorough audit and review of the security and governance, risk and compliance implications of any of the AI solutions used in your organisation before they were deployed?"

ANZ 2025



CYBERSECURITY BREACH DATA & IMPACTS

In comparison to 2024, 2025 data showed slight improvements in the average time to recover post breach and better data recovery rates. However, the disconnect between the time business leaders expect to be back in operation compared to the IT reality persists.

The 2024 disconnect between the time business leaders expect to be 'up and running' after a breach or attack, and the time IT professionals require for recovery still exists in 2025.

24% of leaders say an outage of 1 day or less is tolerable and by the end of day 5, 80% of leaders expect the organisation to have data access restored and be back in business.

The average time IT leaders reported it took to restore a minimal level of business operation? 4 weeks – admittedly an improvement over the 5 weeks reported in 2024, but still a large gap between expectations and reality.

What else did our data tell us?

70% of organisations experienced some form of cybersecurity attack in the last 12 months and almost all of them had been subject to a ransomware demand.

20% paid.

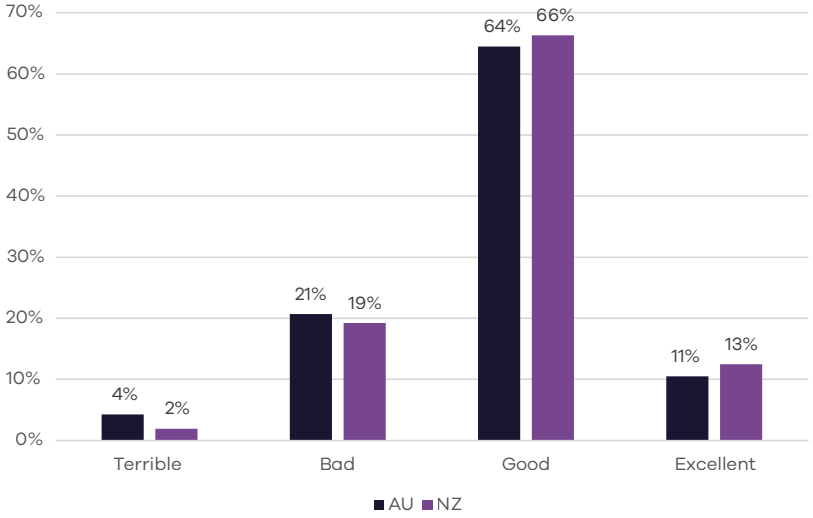
Interestingly, 54% of companies have a 'no payment' ransomware policy and 15% of those still paid, suggesting that reality trumps principles when the inevitable does happen.

Of those attacked:

- 74% experienced data exfiltration;
- 24% of Australian companies and 42% in New Zealand were locked out of their data during attacks;
- 29% in Australia and 36% in New Zealand lost data. Of these, 43%/22% (AU/NZ) recovered 100% of data (compared with 33%/19% in 2024);
- 23% in Australia and 16% in New Zealand experienced no disruption when attacked, 21%/9% (AU/NZ) experienced 'total disruption; and
- 26% of companies found out about their breach when they were unable to access their data. Another 24% found out when contacted by journalists, the attackers, or discovered their data on the dark web. Or to put it differently, 1-in-2 breaches were found by internal tools, systems and third-party cybersecurity partners.

"How would you rate your company's ability to continue operating during a cybersecurity attack that restricted access to important data?"

ANZ 2025



THE RECOVERY AND RESILIENCY ENVIRONMENTS

Testing, testing, testing.

Compared to 12 months ago, companies have made progress strengthening their cybersecurity capabilities:

- 70% of organisations have an incident response plan (up 1% from 2024).
- 8% score themselves as 'very proactive' when describing their cyber resiliency maturity (compared to 3% in 2024). 7% have no clear strategy or capability (11% in 2024).
- When under attack, response rates have improved. 38% of companies now rate their response as 'good' compared to 26% a year ago.
- 1-in-3 ANZ organisations now undertake a 'comprehensive' test of their recovery plans.

However, the data suggests the focus is on the process and not the technology environments, as only:

- 17% test their Active Directory recovery;
- 24% test application recovery;
- 14% test SaaS recovery;
- 22% test system configuration recovery; and
- 12% test meta data recovery.

Our data illustrates how an attack or breach can change an organisation's perspective:

- Companies not attacked scored themselves 'excellent' in their 'ability to maintain business

operations with no disruption' 2.5 times more than those that had been attacked.

- Those attacked were then 1.5 times more likely to undertake (as part of broader reviews) a thorough and complete review of AI tools and solutions compared to those that had not been attacked.
- Companies not attacked were 1.5 times more likely to expect to be back in business within 1 day compared with those that have experienced the reality of an attack.
- Those not attacked rate their expectation of how they would perform if they were attacked as twice as likely to perform well with clearly understood response plans, communications processes and related IRP activities compared to those that have been attacked.

PARTNER ECOSYSTEM SUPPORT

Enhancing capabilities and lifting skills: partners are a critical support option for 9-in-10 organisations.

More data, more regulations, multi-infrastructure environments and, greater demand for stronger operational resiliency – it's no wonder partners are important. When it comes to advice on all things data management, cybersecurity and operational resiliency, the partner ecosystem is trusted by 90% of companies across ANZ.

As with our previous edition, partners were identified as bringing a range of advantages and capabilities including:

1. **Skills availability;**
2. **Infrastructure, cyber operations (and related vendor) management;**
3. **Breach recovery and incident analysis;**
4. **Education and training; and**
5. **Management of governance, risk, and compliance requirements.**

The most trusted type of partner by country can be seen in the table:

Country/ Trust Rank	1	2	3	4	5
Australia	Managed services provider	Strategy consultancy or advisory	Managed security services provider	Telco partner	Systems integrator
New Zealand	Managed services provider	Managed security services provider	Strategy consultancy or advisory	Telco partner	Systems integrator

IN CLOSING

Breached or not breached? That is the question.

Those that have been, perform better the next time around, have higher maturity levels, better expectations around recovery and resiliency capabilities, and more thorough incident response plans and testing baked into their operations.

If you haven't been attacked yet, learn from others.

We're not suggesting organisations are cybersecurity complacent – far from it.

Nor do we believe they are unaware of the complexities of incident responses, testing, business resiliency and recovery activities. However, for those yet to be attacked, the data shows they have higher levels of optimism about their perceived strength of their cybersecurity capability and operational resiliency.

Make sure IRPs don't just cover the process. Expand them to incorporate all aspects of cybersecurity resiliency – workloads, interdependencies, Active Directory, meta-data configurations, etc.

We all know things aren't going to get easier. Government regulations will continue to be 'enhanced', the integration of AI solutions into business operations presents both opportunities and challenges and learning to continuously manage and adapt incident response plans will become more critical.

Lastly, progress is being made with positive results on several fronts including maturity levels, data recovery rates, and recovery times. Closing the gap on expectations that business leaders have for operational resiliency and breach recovery times and the IT reality will serve to reinforce this progress.

COMMVAULT PERSPECTIVE

In the rapidly evolving landscape of business and technology, continuous business operations while maintaining robust cybersecurity is paramount. Organisations must look to adopt a proactive and comprehensive approach to data management, recovery, and cyber resiliency to stay ahead of emerging threats and regulatory requirements. The best practices for continuous business outlined in this report provide a roadmap for achieving these goals.

Robust Data Management and Recovery

Organisations must perform regular testing of their data management, recovery, and cyber resiliency capabilities. This involves implementing a multi-layered security strategy that includes both preventive and reactive measures. Regular testing of these capabilities is crucial to identify and address any vulnerabilities before they can be exploited by cyber threats. By conducting frequent drills and simulations, organisations can build confidence in their ability to respond effectively to incidents and minimise downtime.

Adapting to Changing Regulations

Regulatory requirements are becoming increasingly stringent, and non-compliance can result in significant penalties and reputational damage. Organisations must stay informed about the latest regulatory changes and check that their policies and procedures are aligned with these requirements. This includes conducting thorough audits and reviews of the security and compliance implications of AI solutions before deployment. AI can offer significant benefits, but it also introduces new risks that must be carefully managed.

Enhancing Incident Response Plans

Incident response plans should cover all aspects of cybersecurity resiliency, including workloads, interdependencies, Active Directory, and metadata configurations. A well-designed incident response plan can help organisations quickly identify and contain threats, minimise the impact on operations, and restore services as quickly as possible. This requires a clear understanding of the organisation's IT infrastructure and the interdependencies between different systems and processes.

Building Strong Partnerships

Strong partnerships with managed services providers can provide organisations with access to specialised expertise and resources that may not be available in-house. Managed services providers can offer a range of services, from monitoring and threat detection to incident response and data recovery, helping organisations to maintain a high level of security and compliance.

Commvault plays a significant role in helping organisations achieve these best practices and enhance their cyber resilience through:

Advanced AI-Driven Automation

Commvault's automation capabilities enhance an organisation's ability to detect and respond to threats, activate reliable and rapid recovery, and maintain a strong security posture. Through real-time personalised insights, autonomous recovery testing, and cyber deception and early warning alerts, this is a win for reducing operational costs and technical debt, as well as addressing challenges such as the the gap between business leaders' expectations and the IT reality of recovery times.

Comprehensive Data Protection and Governance

Organisations will continue to navigate the complexities of regulatory requirements, including those related to AI, this year. To support the need for comprehensive data protection as the governance landscape changes, capabilities such as threat scanning, data discovery & security audits, as well as cleanroom recovery become critical to any organisation's cyber resilience strategy. As an example, Commvault's assessment of it's SaaS platform at the Protected level of the Infosec Registered Assessor Program (IRAP) demonstrates commitment to meeting the highest security and integrity protocols aligned to the Australian government's information security standards.

Unified Approach to Cyber Resilience

Maintaining operations during and after cyber attacks is certainly easier said than done. Enhancing incident response planning and cybersecurity maturity through a platform that unifies capabilities such as end-to-end observability, a hardened security posture, and a security scorecard will greatly contribute to a robust cyber resilience strategy.

The recommendations outlined in this report emphasise the importance of strong incident response planning, thorough data management, and compliance with regulatory requirements. This is particularly relevant in the context of constant technology and industry landscape changes advanced by an increasing number of cyber events. Strength in cyber resiliency will take a combination of people, process, and technology to achieve continuous business operations.

APPENDIX

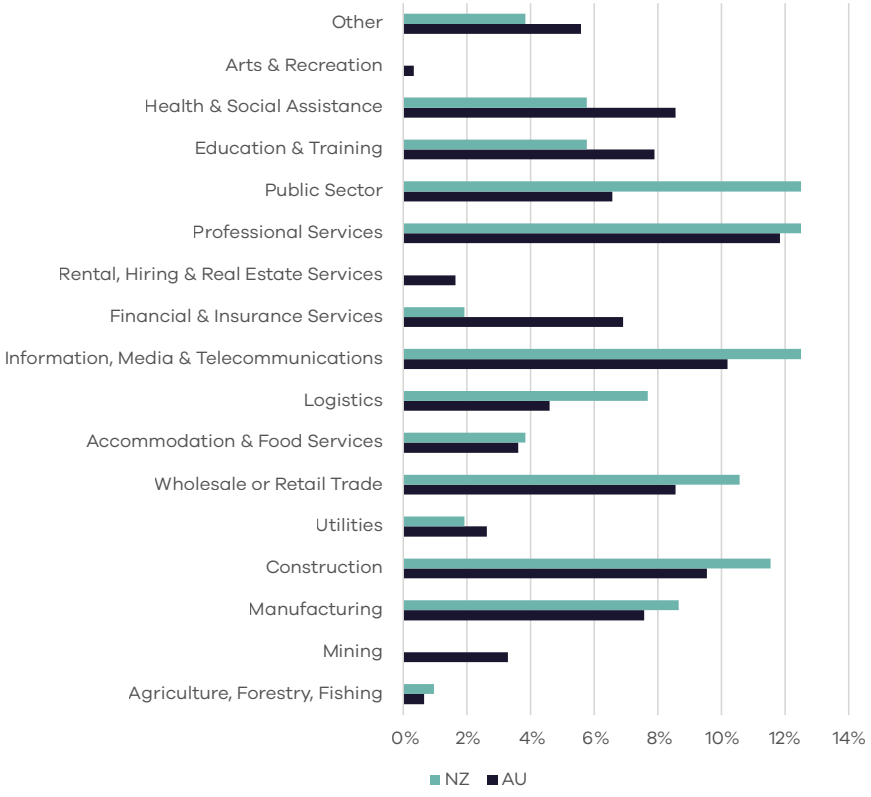
The research methodology and demographics

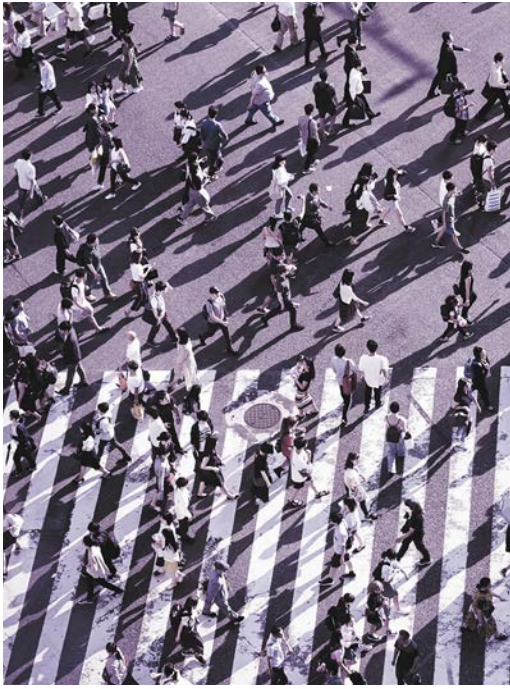
Using an online panel, TRA conducted an independent quantitative market research survey in December 2024 and January 2025.

The total sample size is 408 organisations (304 in Australia and 104 in New Zealand) and respondents were CIO/CISO, IT Leader, IT decision marker 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 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.

ABOUT TECH RESEARCH ASIA (TRA). TRA is a fast-growing IT analyst, research, and consulting firm with an experienced and diverse team in: Sydney | Melbourne | Singapore | Kuala Lumpur | Hong Kong | Tokyo. We advise executive technology buyers and suppliers across Asia Pacific. We are rigorous, fact-based, open, and transparent. And we offer research, consulting, engagement and advisory services. We also conduct our own independent research on the issues, trends, and strategies that are important to executives and other leaders that want to leverage the power of modern technology.

www.techresearch.asia

Commvault®

TRA