Insight Commvault

CYBER RESILIENCY EDITION

Australia & New Zealand

February 2024

A Tech Research Asia Insights Report,
commissioned by Commvault.

TRA

INTRODUCTION

Welcome to our 4th edition of The State of Data Readiness in ANZ

Businesses in Australia and New Zealand (ANZ) face complex data, security and regulatory environments. As regulatory requirements continue to focus on protecting consumers and citizens, the onus on companies to secure, protect and recover (if breached) their data environments grows increasingly challenging.

In the event of a breach or cyber security incident (an increasingly common experience for many businesses), executives expect minimal disruption to business operations. Technology and cyber security professionals also know that the reality of the time taken to return to business-as-usual operations is somewhat longer.

When asked how long they can wait to be back in business after an incident, business leaders say 'days'. Tech folks reply 'weeks or months... maybe'.

This tension between expectations and reality has heightened the focus on enhancing cyber resiliency capabilities.

Organisations are looking to create or strengthen their ability to continue business operations and deliver outcomes even when experiencing cyber attacks and to eliminate, or at least substantially reduce, recovery delays if breached.

Reflecting this focus on cyber resiliency, this report explores a number of topics including:

- **Data growth, infrastructure, and dark data issues;**
- **Breach recovery of data and performance;**
- **Cyber resiliency maturity levels;**
- **The use of AI solutions in offensive and defensive cyber security operations; and**
- **Considerations for strengthening and enhancing cyber resiliency capabilities.**

We hope that you find value in comparing your organisation to your peers in Australia and New Zealand, and that the insights in this report help you to enhance and strengthen your own data management, recovery, and cyber resiliency capabilities.

Sincerely,

Tech Research Asia

The data provided in this Commvault commissioned TRA Insights Report comes from 400 companies in Australia (300) and New Zealand (100). Additional information on this sample can be found in the appendix of the report.

HIGHLIGHTS FROM THIS REPORT

- There is a significant disconnect between business expectations and technology reality when it comes to restoring business operations if breached.
- The research data shows that companies are not recovering all their data, nor can they maintain business operations when breached.
- There is an inevitability to being breached and cyber resiliency is critical.
- Threat actors target a mixture of data environments, increasingly looking at production + secondary + backup estates as a 'nuclear' option.
- Cyber resiliency maturity is low and organisations continue building and enhancing their capabilities.
- Immutability, cleanrooms, AI and partners can help bolster cyber resiliency effectiveness.

DATA ESTATES

Growth and waiting for AI

On average, companies in ANZ saw their data estates grow by 24% in the last 12 months, down from the 40% growth recorded when we started this research in 2020.

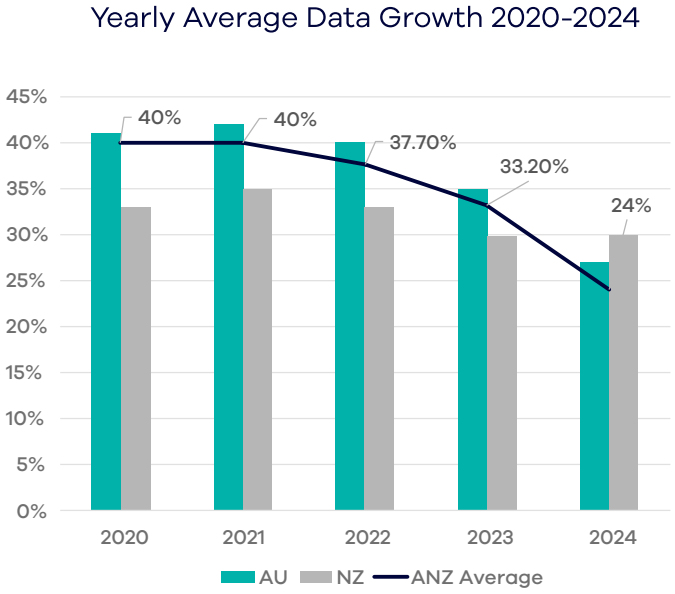
Similar to our 2023 report, the primary drivers for this lower growth rate can be mainly attributed to 3 key factors:

- **A focus on limiting or lowering risk exposure (through reducing the amount of data retained that could be exposed by a cyber security breach);**
- **Optimisation of storage technologies to shrink data estates; and**
- **A need to reduce, or at least slow the growth, in costs of storing, securing, and managing data as regulatory requirements continue to push organisations to ensure compliance.**

6% of Australian firms (4% in 2023) and 9% of New Zealand firms (5% in 2023) reduced their data estates by an average of 20% in the preceding 12 months.

Our research indicates that 51% of ANZ companies have established strategies to protect data and content created by generative AI (Gen-AI) solutions.

We are curious to see the impact of this on data growth in the coming 12 months and our current view is that growth rates of stored data will again accelerate as gen-AI content is created, stored, and secured.


Yearly Average Data Growth 2020-2024
45%
40%
35%
30%
25%
20%
15%
10%
5%
0%
40%
40%
37.70%
33.20%
24%
2020
2021
2022
2023
2024
AU
NZ
ANZ Average

DATA ESTATES

Data infrastructure and dark data

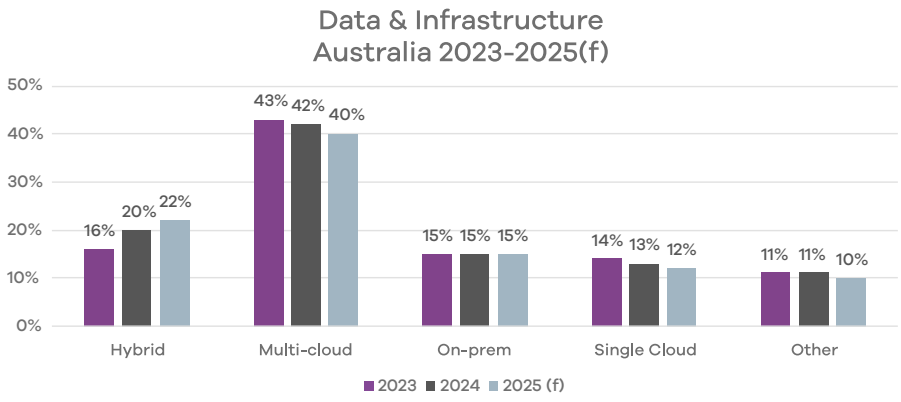
Infrastructure continues to be cloud-centric and dark data challenges are rising

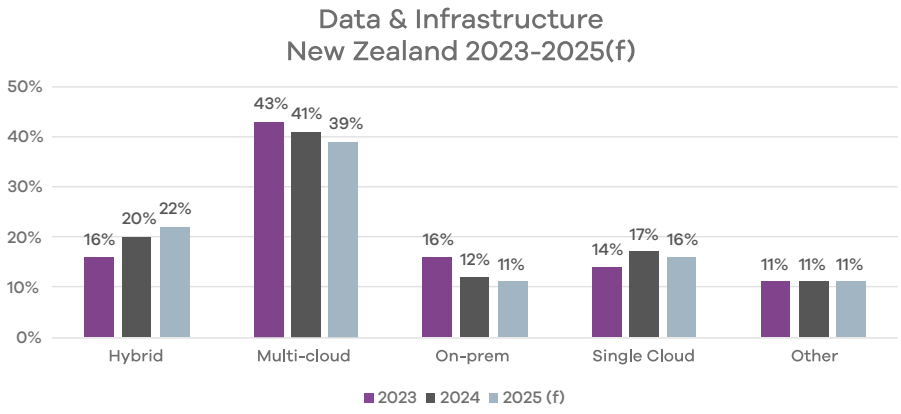
On average, 63% of companies in ANZ continue to use 'blended' environments (mixing either cloud or cloud and physical infrastructure), for their data estates. This represents an increase of 16% since 2020 (when it stood at 47%).

Between 2020 and now, the percentage of companies solely using on-premises infrastructure has stabilised at an average of 14% in 2024, down from 21% in 2020.

Regardless of location, data sprawl through multiple infrastructure environments brings increased complexity, disparate tool sets, and potential for delays in investigating cyber security incidents and recovering from data breaches.

With infrastructure sprawl challenges increasing, we were not surprised that our data showed an increase in the number of companies struggling to manage dark data (i.e. data that is created and unmanaged or sits outside of the businesses' scope of management control and/or visibility), rising from 73% in 2023 to 84% in 2024.





"Using multi-infrastructure to support data and workloads is default for many organisations and the benefits are clearly established. It becomes problematic when you need to use multiple tools across multiple clouds – it's messy, complex, and inefficient. You lose the context of the data and when there's a cyber incident, it's much harder to understand the nature of the threat and to quickly recover."

Craig Bastow
Country Manager – Australia and New Zealand, Commvault

THE TOP 2 ISSUES IMPEDING DATA MANAGEMENT & SECURITY

Recoverability, we have a problem...

Alongside data/infrastructure sprawl and dark data, the top 2 operational challenges organisations cited in managing and securing their data environments are:

1. **Effective and speedy data recovery after a cyber security incident; and**
2. **Establishing a robust cyber resiliency capability**

Let's dig a little more deeply into these 2 issues, starting with data recovery after a breach.

Business expectations for recovery time don't align with technology reality

Our research reveals a substantial 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.

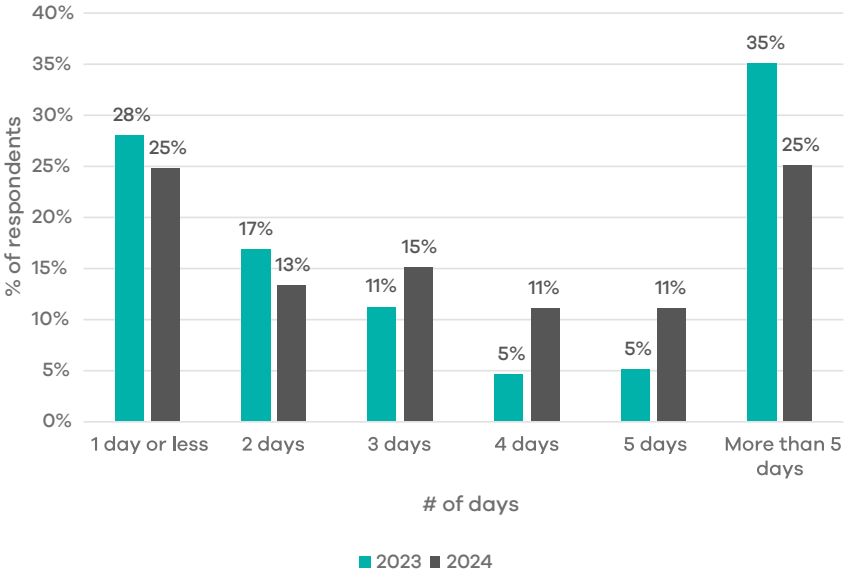
For business leaders, speed of business resumption is the critical factor – 25% of leaders say an outage of 1 day or less is tolerable. By the end of day 5, 75% of leaders expect the organisation to have data access restored and be back in business, an increase of 10% over 2023.

Let's be clear, 75% of business leaders want to be back in business after a cyber incident in **5 days or less.**

The average time IT professionals in our research reported it took to recover from a breach? **5 to 8 weeks (and 30% took more than 3 months).**

Plainly, there's a problem between business expectations and IT reality.

From your perspective as an executive business leader, how long could your business tolerate an outage with restricted access to critical data?
ANZ, 2023-2024



BREACH RECOVERY

3 Things Business Executives Need to Consider

The '5 days versus 5-8 weeks' difference is challenging, and it helps to understand some of the common issues our research revealed that contribute to the complexity of recovery, namely:

1. **It's not just 'one thing' that gets targeted in an attack – recovery spans production, secondary, and backup environments;**
2. **The 'cloud' brings benefits but also has limitations; and**
3. **Just because a company has an incident response plan doesn't mean it works.**

Have you been attacked?

62% of Australian and 68% of New Zealand organisations stated they had been subjected to at least one cyber attack in the last 12 months, a figure comparable to our 2023 data.

Troublingly, of the ANZ companies in 2024 that were attacked, 10% of these were unaware of what had been targeted and if data had been exfiltrated.

On a more positive note, compared to 2022 data, the percentage of companies breached and losing data decreased in 2024 for both Australia and New Zealand, down to 55% and 43% respectively (from 72% and 48%).

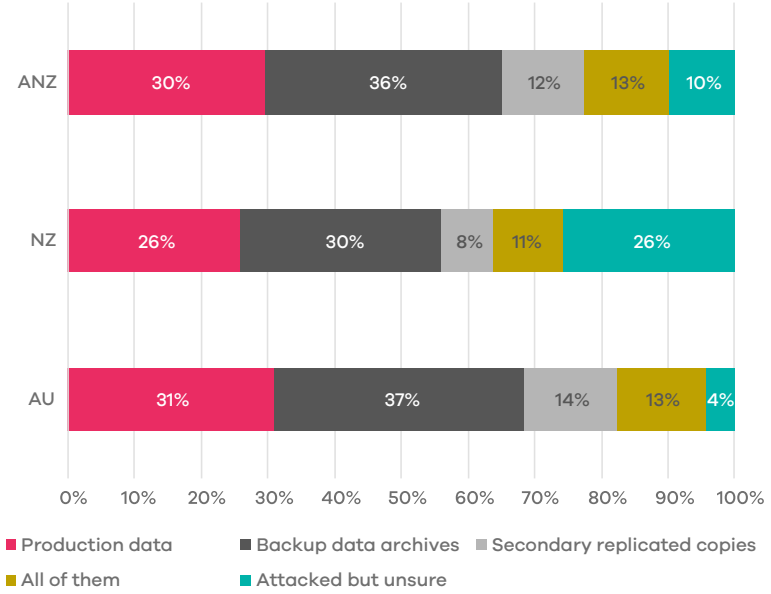
These attacks do not simply target one part of the infrastructure that supports business operations, for example, just the production environment. Increasingly, attacks are multi-faceted, targeting 2 or more areas such as production and backup, or production and secondary. On average:

36%
of attacks started by targeting backup data;

30%
targeted production data; and

13%
targeted all 3 areas.

Thinking about the most recent cyber attack your company experienced, did it start by targeting...?



BREACH RECOVERY

Cloud – it's both good and bad

Having a blended, multi-infrastructure environment provides flexibility and scalability.

An average of 74% of companies (83% in Australia and 70% in New Zealand) indicated they are either using, or intend to use, cloud services in the next 12 months to manage and secure their multi-infrastructure environments.

The potential problem here is that using cloud native tools (e.g. Azure tools for Azure, AWS for AWS, GCP for GCP, etc.) can create inefficiencies.

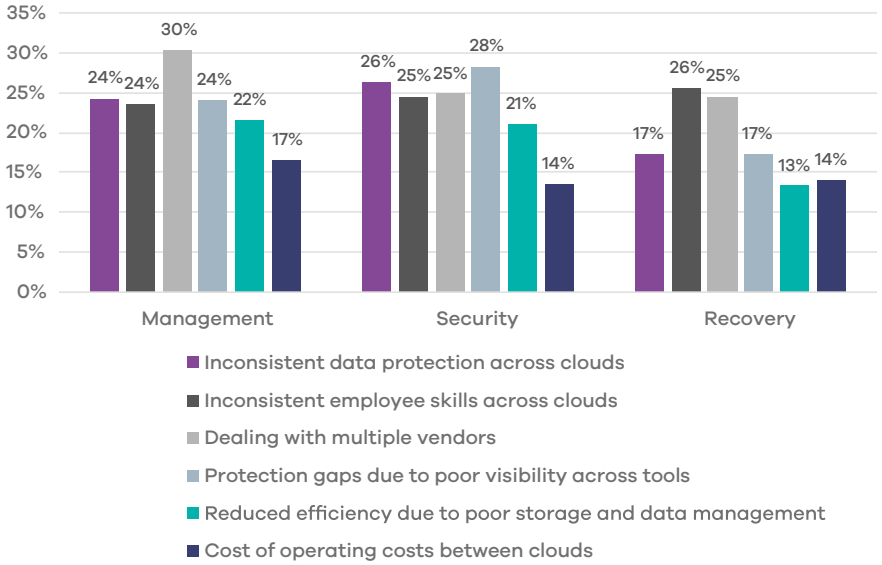
Each tool is optimised for its own infrastructure. This makes it difficult to create a standardised data management platform that works effectively across multiple environments. Extending further into physical, on-premises as well as cloud only exacerbates the issue.

Looking across the research data reveals that:

- **Management is complex:** 30% of companies experience problems managing data with multiple vendors across multiple environments, 24% highlighted difficulties both with managing data and protection gaps and inconsistent employee skills.
- **Securing is sub-optimal:** 28% experience protection gaps because of poor interoperability between different cloud tools, 26% have inconsistent data protection between clouds, and 25% point to inconsistent employee skills.
- **Recovery is adversely impacted:** 26% state that inconsistent skills sets across clouds hampers recovery, as does dealing with multiple cloud vendors for 25%, and 17% point to inconsistent data visibility and protection between infrastructure.

In these circumstances, variable data protection capabilities across environments increase the pressure on businesses to have consistent skills to address each appropriately, and arguably, look to an integrated, single platform approach that offers skills harmonisation, visibility, insight and improved recovery capabilities.

What are the top challenges you face using native data management, security and recovery tools in a multi-infrastructure environment?
ANZ



BREACH RECOVERY

You have an incident response plan. But when did you properly test it?

On average, 69% of ANZ companies (71% in Australia, 60% in New Zealand) stated they have an incident response plan that is used to support their response and recovery activities if attacked. A commendable 62% state they test their plans at least every six months...

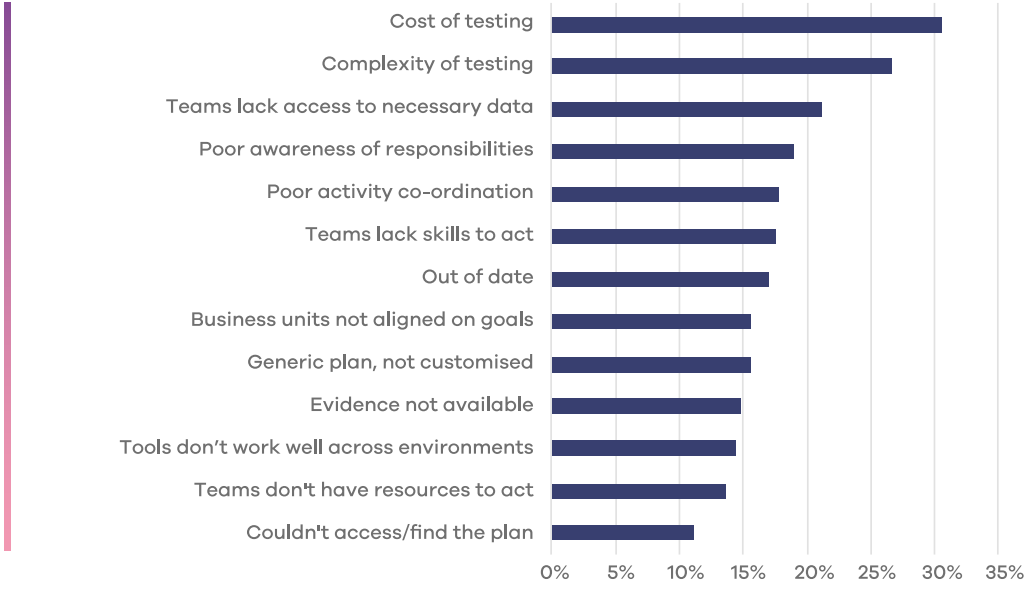
We suspect that 62% represents a 'table-top' test, rather than a proper response. Otherwise, if companies were truly testing their plans diligently, why is it when asked about their incident response performance, 23% stated "we scramble to respond and our response is poor" and another 56% said "We could do better"?

Active testing is very different to a 'table-top' review. Our research revealed a number of problems that make companies reluctant to vigorously test their plans, including:

- **Cost;**
- **Complexity;**
- **Teams not having the right skills to act on testing the plan;**
- **Poor responsibility awareness; and**
- **Poor co-ordination.**

Worryingly, 12% of companies stated they couldn't find or access the plan to test it, despite having one prepared.

What problems do you experience when testing your incident response plan?
ANZ



CYBER ATTACKS

Data recovery rates & breach awareness

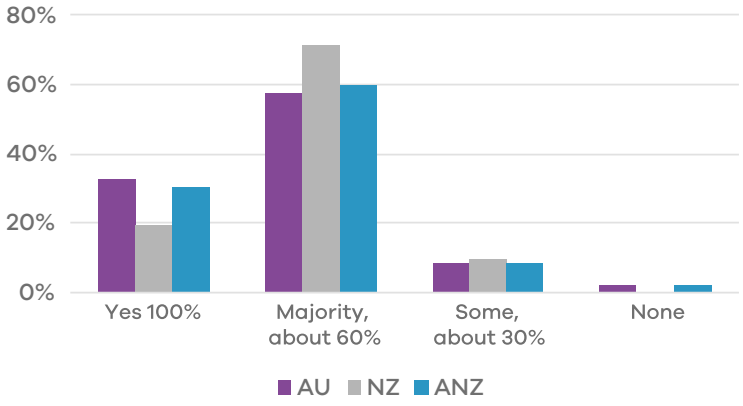
As noted earlier, more than 6-in-10 ANZ organisations had experienced at least one cyber attack in the last 12 months. Did they recover all their data?

Not quite.

33% of Australian and 19% of New Zealand companies stated they successfully recovered 100% of their data. This represents declines from 2020 when the average 100% recovery rates sat around 50% for ANZ.

Businesses need to move beyond 'are backup jobs running?' to a more proactive stance to ensure compromised data is 100% recoverable and have solutions like data cleanrooms and immutability in place to support this.

You stated your company was targeted in a ransomware attack and suffered a data breach or loss. Did you completely recover your data?
ANZ

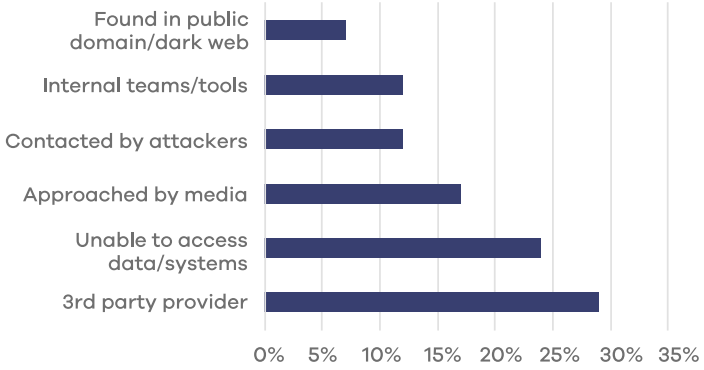


How did companies discover they had been breached?

Pointing to the importance of having strong security partners, the most common way companies discovered they had been breached was informed by their 3rd party security providers (29%).

- 36% found out from other external activities (approached by media – 17%, contacted by attackers – 12%, found their data in the public domain or dark web – 7%);
- 24% became aware when they were unable to access their data or systems; and
- 12% from their internal teams or security tools.

You stated your company was targeted in a ransomware attack and suffered a data breach or loss. Did you completely recover your data?
ANZ



CYBER SECURITY = CYBER RESILIENCY

Not really.

Let's explore the 2nd issue organisations identified that has a direct impact on effective and speedy business recovery – cyber resiliency.

Isn't cyber resiliency the same as cyber security?

No. Cyber security concentrates on creating and maintaining an overall approach that protects digital assets.

The US National Institute of Standards and Technology (NIST) defines cyber security as "The ability to protect or defend ... from cyber attacks". Broadly, it focuses on prevention via tools such as firewalls, encryption and antivirus, with the aim of addressing threats (internal and external) to prevent breaches and unauthorised access.

Resiliency has a number of key differences, starting with the NIST definition: "The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources[1]."

As such, cyber resiliency focuses on adaptability and recoverability, through strong incident response plans, backup and recovery systems, and incorporates business continuity, risk management and training. Rather than prevention, resiliency focuses on continuity even if breached, assuming that attacks and breaches are inevitable.

How mature are ANZ companies when it comes to cyber resiliency?

Frankly, we were a little surprised by the data showing that more than 50% of ANZ organisations have a very immature cyber resiliency capability. Currently an average of 4% of ANZ companies believe they have

"Cyber resiliency is an ongoing journey. It's a combination of people, processes, and technologies that you're continually evolving and testing to ensure the integrity of your business."

Craig Bastow
Country Manager – Australia and New Zealand, Commvault

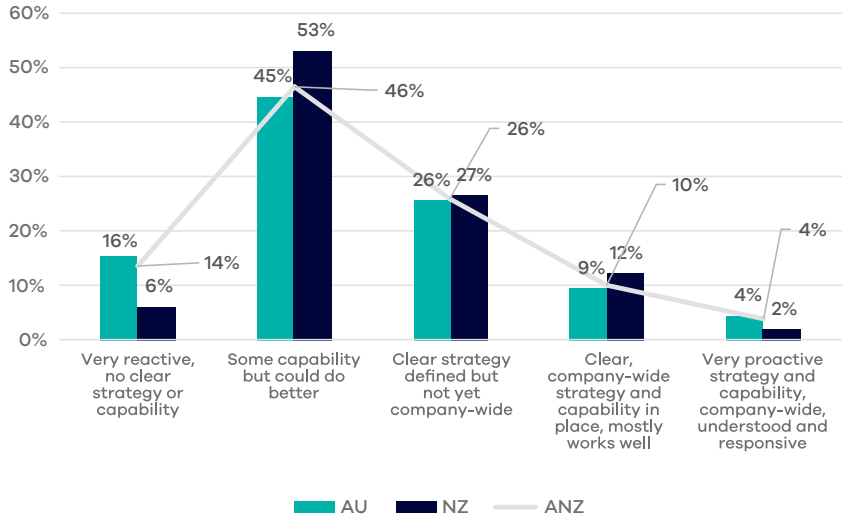
a proactive, mature, cyber resiliency capability, and another 10% point to a 'clear, company-wide strategy that mostly works well'.

Companies in ANZ are very well versed and, mostly proactive when it comes to developing and implementing cyber security protection.

We believe the lower levels of self-assessed resiliency maturity reflect the deep levels of awareness of cyber security capabilities and the pragmatic understanding of the steps necessary to create the same levels of mature resiliency.

[1] Source: https://csrc.nist.gov/glossary

Thinking about cyber resiliency maturity, which of the following statements best describes your company's maturity level?
ANZ



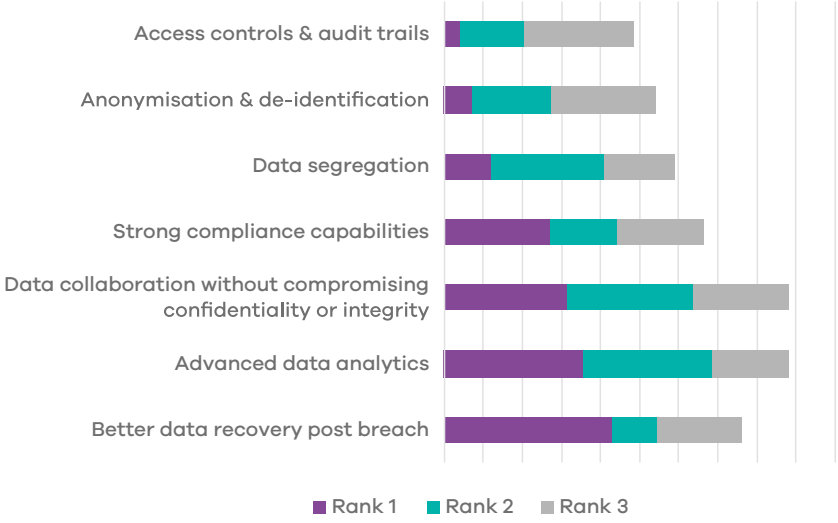
STRENGTHENING RECOVERY AND RESILIENCY

Some quick wins to bolster capability

As part of this research, we asked organisations what other investments or initiatives are considered important to recovery and improving cyber resiliency. Four key areas were identified:

1. **Data immutability.** Increasingly important for organisations seeking cyber risk insurance, having an immutable copy of data provides for quicker recovery, better data integrity and compliance, and more effective auditing and forensic capabilities. However, maintaining immutable data across multi-infrastructure environments that doesn't impact system performance and increase data management complexity was identified as the top challenge for organisations when trying to secure their data estates.
2. **Data cleanrooms.** 80% of ANZ companies are using data cleanrooms (82% in Australia and 74% in New Zealand), highlighting some key advantages they bring to their recovery and resiliency stances:
   - Better data recovery post breach;
   - Advanced analytics supporting forensics;
   - Data collaboration; and
   - Compliance.
3. The adoption of **artificial intelligence** for cyber security.
4. Using **partners** to enhance skills and response capabilities.

Please rank the top 3 benefits your company gets from using data cleanrooms where 1 is 1st benefit, 2 = 2nd, etc.
ANZ



"We're seeing companies faced with a scenario where recovering little bits and pieces as they would do in an operational recovery simply does not work. Now, they have to recover everything at once. The ability to recover at scale is hugely important. Cleanrooms give customers that."

Craig Bastow
Country Manager – Australia and New Zealand, Commvault

AI FOR CYBER SECURITY AND RESILIENCY

Offensive or defensive AI, or both?

The third area identified in our research is the adoption of AI solutions to strengthen cyber capabilities.

Much has been written about the growth of generative and other artificial intelligence solutions in the cyber and broader technology arenas. We're not going to add to that here.

Rather, we wanted to explore if companies were adopting AI for cyber security and if so, was the focus more offensive or defensive in intent?

We learnt that 55% of companies are either using AI, or plan to use in the immediate future to support their cyber security and resiliency. On average in ANZ, of those using AI:

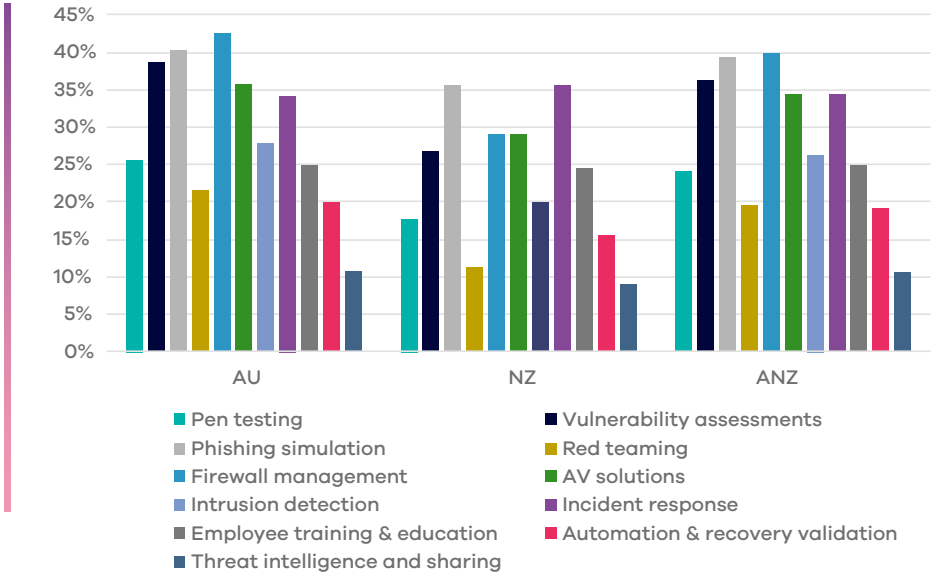
41%
are using it offensively with phishing simulation being the most popular application;

32%
are using it defensively with antivirus the main application;

27%
are using it for both offensive and defensive purposes; and

28%
currently have no plans to use in the next 12 months.

Where do you use AI tools in your cyber security and data protection environments?



"AI is becoming an integral component of cyber resiliency, helping organisations manage and respond to threats that span multiple data infrastructures, SaaS services, virtual environments and more."

Craig Bastow
Country Manager – Australia and New Zealand, Commvault

PARTNER ECOSYSTEM SUPPORT

Enhancing capabilities and lifting skills

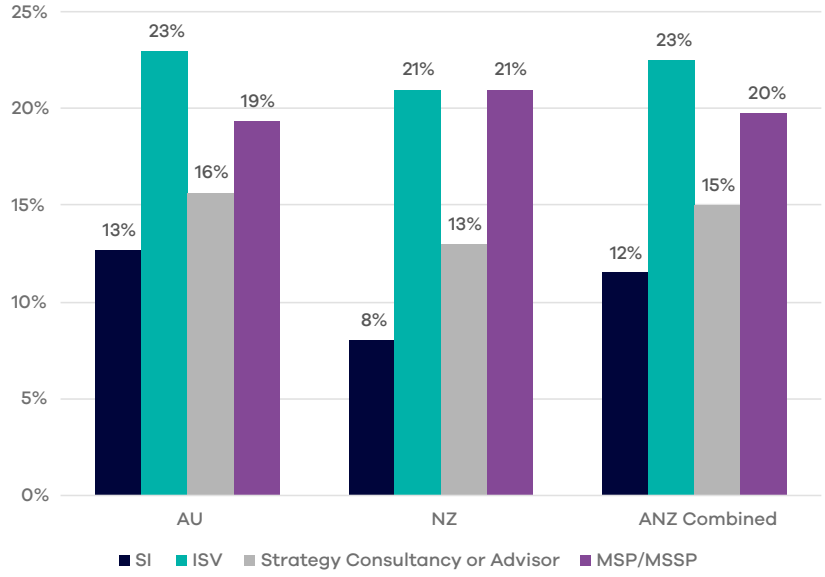
On average 94% of ANZ companies (95% in Australia and 93% in New Zealand) engage technology partners in some way to support data management, security, and recovery operations.

Partners were identified as bringing a range of advantages and capabilities with the top 5 being:

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.**

In ANZ, managed services (MSP)/Managed Security Service Providers (MSSP) are the 2nd top preferred choice for 20% of ANZ organisations, alongside cyber security advisory firms (23%), and independent software vendors (ISV, 15%).

What type of technology partner is your preferred choice for your company's data management and cyber security initiatives? (Top 4 partner types only shown)



IN CLOSING

We sincerely hope you found value in the report and the analysis helps you to continue enhancing your recovery and resiliency capabilities.

The data shows that companies are recovering less of their data when breached and taking longer to recover it and get back to business.

Cyber resiliency is now a key consideration for companies. Our research shows that organisations are facing a 'when, not if' scenario of suffering a cyber security breach and there is a significant disconnect between business expectations and technology reality when it comes to restoring 'business as usual' operations.

In support of these initiatives, organisations are looking to increase their investment in creating immutable data copies, establishing cleanrooms that are part of integrated data management, backup and resiliency platforms, whilst exploring the use of both offensive and defensive AI for cyber security.

COMMVAULT PERSPECTIVE

In today's complex and ever-evolving cyber landscape, organisations must prioritise cyber resilience to ensure the continuity of their business operations and protect their valuable data. The State of Data Readiness Cyber Resiliency Edition report for ANZ highlights several best practices that can help organisations enhance their cyber resilience capabilities. These best practices include:

Establishing a Proactive Platform-based Cyber Resiliency Strategy across your Enterprise: Organisations should develop a comprehensive and proactive cyber resiliency strategy that focuses on anticipating, withstanding, recovering from, and adapting to adverse conditions, stresses, attacks, or compromises. This strategy should align with the organisation's overall business objectives and incorporate strong incident response plans, backup and recovery systems, and business continuity measures.

Bridging the Gap between Business Expectations and Technology Reality: There is often a disconnect between the time business leaders expect to be back in business after a breach and the time IT professionals require for recovery. Organisations should bridge this gap by setting realistic expectations and investing in technologies and processes that enable faster recovery times. This may include leveraging technologies like data cleanrooms, immutability, and artificial intelligence to enhance data recovery and integrity. The ability to recover at scale is critical and companies must ensure they take a platform approach that integrates all aspects of backup, recovery and resiliency.

Embracing Data Immutability: Data immutability, or the ability to maintain an unchangeable copy of data, is becoming increasingly important for organisations seeking cyber risk insurance. Immutable data provides quicker recovery, better data integrity and compliance, and more effective auditing and forensic capabilities. Organisations should invest in solutions that enable data immutability across multi-infrastructure environments without impacting system performance or increasing data management complexity.

Implementing Data Cleanrooms: Data cleanrooms are controlled environments that allow organisations to securely analyse and manipulate sensitive data without compromising its integrity. These cleanrooms can significantly enhance data recovery post-breach, improve data integrity and confidentiality, and support advanced analytics for forensics. Organisations should leverage data cleanrooms to strengthen their recovery and resiliency stances. Lastly, cleanrooms create an environment where regular testing of incident response and recovery plans can be undertaken cost efficiently and with minimal disruption to business operations.

Leveraging Artificial Intelligence for Cyber Security: Artificial intelligence (AI) can play a crucial role in strengthening cyber security and resiliency. Organisations should adopt AI solutions that can help them detect and respond to cyber threats more effectively. AI can be used defensively for tasks like firewall management and offensively for activities like phishing simulation. By leveraging AI, organisations can enhance their cyber security capabilities and stay one step ahead of cyber attackers.

Engaging Technology Partners: Organisations should collaborate with technology partners to enhance their data management, security, and recovery operations. These partners can bring valuable skills, infrastructure management capabilities, breach recovery expertise, education and training, and governance, risk, and compliance management. Organisations should carefully select partners based on their specific needs and preferences.

By implementing these best practices, organisations can strengthen their cyber resilience capabilities and better protect their data and business operations. It is crucial for organisations to bridge the gap between business expectations and technology reality, embrace technologies like data immutability and cleanrooms, leverage AI for cyber security, and engage with trusted technology partners. These practices will help organisations minimise the impact of cyber attacks, and ensure the continuity of their business operations in the face of evolving cyber threats.

APPENDIX

The research methodology and demographics

Using an online panel approach, TRA conducted an independent quantitative market research survey in December 2023 and January 2024.

The total sample size is 400 organisations in Australia and New Zealand and respondents are CIO/CISO, IT Leader, IT Decision Maker and direct reports.

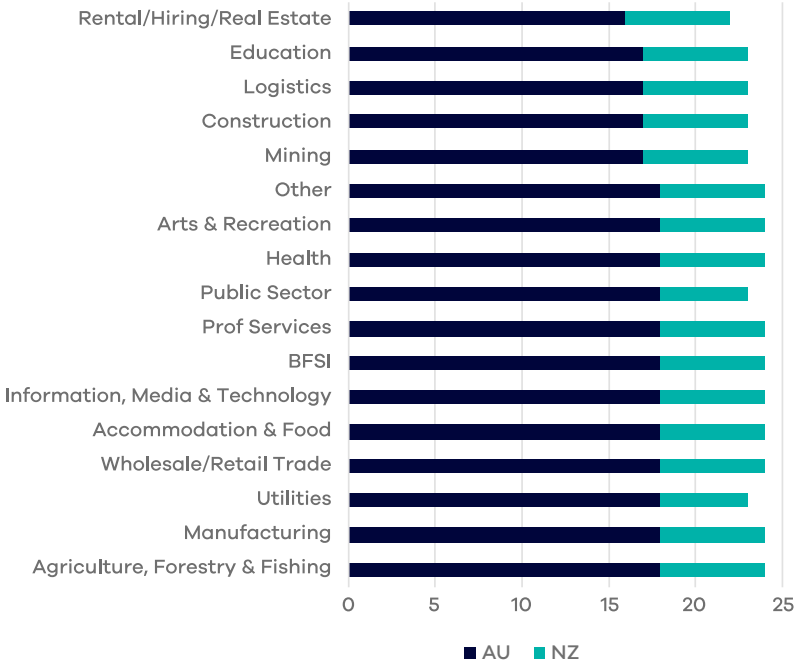
Company size by employees:

Australia
100-199: 153 (51%)
200+ : 147 (49%)

New Zealand
50-199: 52 (52%)
200+: 48 (48%)

Country distribution:
Australia: 300
New Zealand: 100

Respondent Company by Industry Sector



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.

For more information email: **Marketing.APAC@insight.com**

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

Insight Commvault

TRA