ANZ Market Analysis: The State of Data Readiness

3nd Edition

February 2023

Authored by TRA TECH RESEARCH ASIA

Commissioned by COMMVAULT®

Introduction & Executive Summary

This is the third edition of Commvault's annual State of Data Readiness report for Australia and New Zealand. Previous editions pointed to the complexity of managing data in multi-cloud environments, the prevalence of cyber security attacks and how organisations were approaching their data management issues during a time of digital transformation.

These issues continue to trend in the 2023 report however we have seen improvements in key areas such as data protection and effectiveness of cloud data management that suggest organisations are making progress.

Key findings for 2023 report include:

1. **A blended infrastructure environment continues to be the default choice for data storage with 62% of all respondents using multi-cloud or hybrid infrastructure.**
2. **Regulatory requirements continue to challenge businesses. For example, 72% of companies are facing changes in their regulatory and legislative environments in the coming 12 months and 58% of companies are already subject to data sovereignty regulations.**
3. **Having too many data sources and growth in unstructured data are the two most significant operational data management challenges.**
4. **65% of companies state their operations could not last longer than 5 days if subject to a business outage that restricted access to critical data.**
5. **Only 40% of survey respondents reported that they could recover 100% of their data after being subject to a ransomware attack.**
6. **Recovery times post cyber attack have increased with 42% of companies in 2023 recovering within 4 weeks compared to 71% in 2021 for the same duration.**

There are three key sections to this report:

1. **Data growth, storage and infrastructure**, providing insights into data growth, the infrastructure used to support companies' data environments, the pros and cons of using cloud infrastructure and the operational challenges of data management.

2. **Data management responsibilities, plans and issues**, focusing on the prevalence and effectiveness of data management plans (DMPs), which role holds the formal responsibility for data management and the impact of regulatory and legislative changes.

3. **Data breaches, losses and recovery**, including average recovery times, impacts of an outage and how companies discover they have experienced a data loss.

The data presented in this edition is drawn from a survey of 376 businesses across Australia and New Zealand (for more information please see the 'About' section at the end of this report).

We hope the report provides you with insights into how your peers are addressing data management issues in the current market environment.

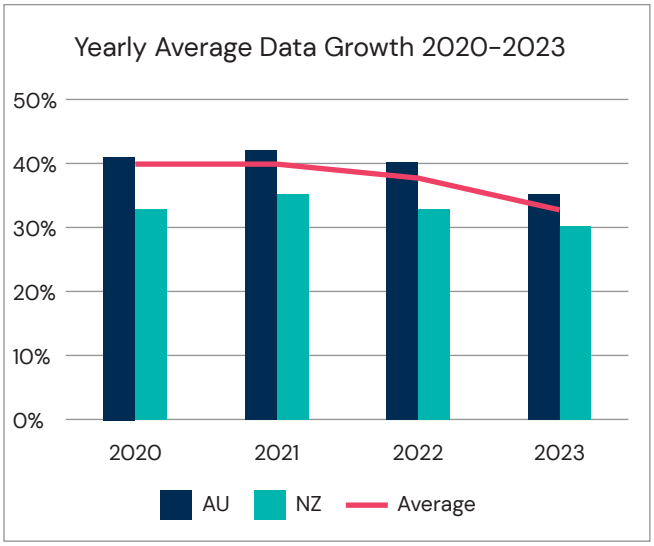
Trends in Data Growth and Storage Infrastructure

Key findings

1. **Annual data growth rates have slowed, down from 40% in 2020 to 33% in 2023 with unstructured data constituting the largest component.**
2. **62% of all respondents are using multi-cloud or hybrid infrastructure to support their data estates.**
3. **Usage of cloud services for data management is high, and organisations need to be aware of the limitations of cloud-native tools tied to specific clouds.**

Data Growth

The research shows that yearly data growth rates between 2020 and 2023 experienced a decline, dropping from 40% annual growth in 2019-20 to 37% in 2021-22 and 33% in 2022-23.



The 2nd edition of this report in 2022 attributed data growth between 2020 and 2022 to a mix of factors including supporting remote working environments and a surge in digital transformation programmes creating more data.

Research for this report edition indicates the possible start of a trend amongst organisations to be more considered with data and information that is gathered and retained. High profile data breaches in 2022 have no doubt contributed to this trend however we also see other significant factors at play:

- **Growth in data storage costs (notwithstanding pricing reductions in some storage options).**
- **Optimisation of storage technologies to shrink data estates.**
- **A greater strategic evaluation of data value, rather than the 'land grab' approach evident by some companies in the past.**
- **Greater understanding of the trade-offs between risk mitigation and data retention leading to elimination of 'no-value' data.**

Notwithstanding this slight decline, data growth remains above 30% and unstructured data forms a large proportion of the total increase. In fact, since the first report, unstructured data as a percentage of the total data created has been relatively constant: 79% for 2022-23, compared to 2021-22 (78%) and 2020-21 (80%).

Whilst organisations continue to experience high levels of unstructured data, they have also been addressing an additional issue around data visibility – dark data. Dark data (i.e., data that is created and unmanaged or sits outside of the businesses' scope of management control and/or visibility) continues to be problematic for many organisations.

The ANZ average shows that 73% of all organisations experienced this problem, with 72% of Australian companies reporting difficulties and a slightly higher 77% of firms in New Zealand.

Data Infrastructure

Our research continues to show a trend of companies using multi-cloud or hybrid environments with just over 62% of our respondents showing a preference for these infrastructures compared to alternatives (such as on-premises, co-location, single cloud, etc.).

The below chart shows the trend over time towards cloud-centric infrastructure, away from purely physical or single-cloud approaches. Between 2020 and 2023 organisations using hybrid or multi-cloud infrastructure has increased from 47% to 62%.

In the same period, usage of single cloud environments and other physical infrastructure have decreased, falling from 53% in 2020 to 37% in 2023. Interestingly, the data also shows that this decline appears to have flattened in the period between 2022 and 2023 and our expectations are that 2024 data will not show significant variation.

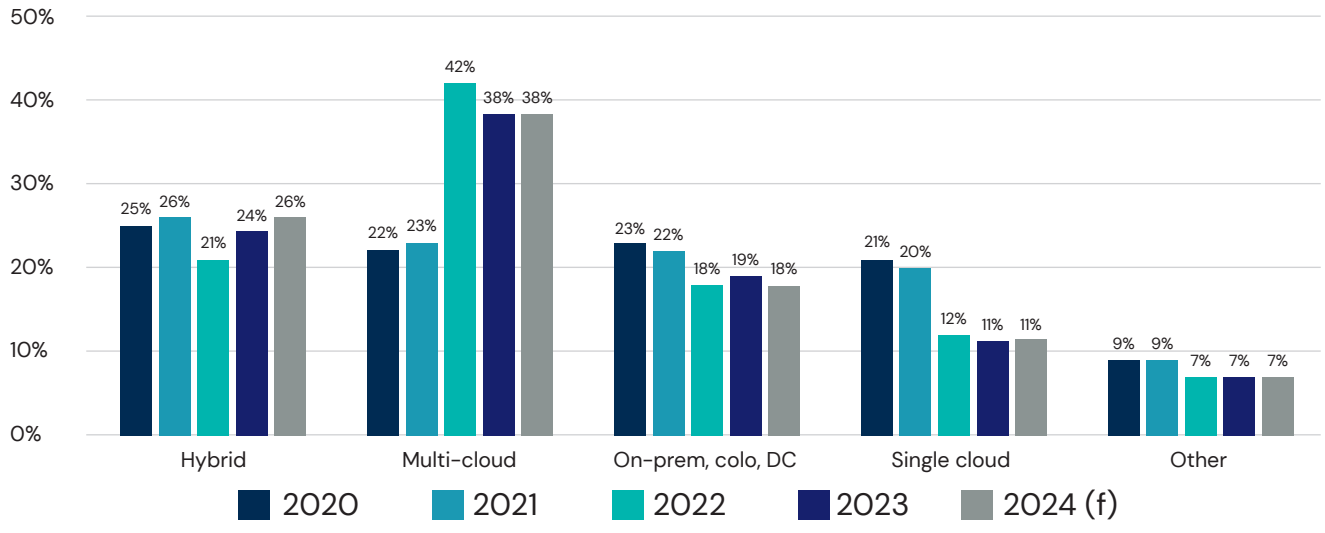
As noted in earlier editions, the growth in data (especially unstructured and dark), deployment across multiple locations, and adoption of multiple toolsets to manage individual environments can exacerbate problems with data sprawl, management complexity, and cyber security.

The Commvault Perspective

There is a clear trend of businesses assessing their data estates and being more proactive with ensuring a 'best-fit infrastructure' with the right data in the right cloud (or on-premises). Compared with the 'just get the data into the cloud' approach of the past, it is clear ANZ organisations are taking a considered and mature approach to leveraging multi-cloud infrastructure.

The increased prominence and breadth of data regulation and legislation is leading companies to focus more intelligently on their data management strategy, capabilities, and technology. Businesses now run on data and, as digital transformation activity continues, they need to ask how they can ensure the fundamental integrity of their business when its existence depends on the data that has been created.

Thinking about the data your company currently manages, please estimate the percentage of data stored in each of the following locations now (2023) & in 12 months' time (2024 f)



Common Data Management Challenges

For 2023, the survey data identified the following top 5 data management challenges faced by companies in Australia and New Zealand (for consistency we continue to use the same definitions from previous reports):

1. **Data storage optimisation.**
   The location, structure, and accuracy of data makes it difficult to manage storage costs, find the right data at the right time and extract value, potentially even more so in a hybrid or multi-cloud environment. (2022 rank: 2)

2. **Data classification.**
   With growth in unstructured data, the ability to organise data by relevant categories becomes significantly more challenging. Poor classification can impede business operations, for example, through increased storage costs or creating security and compliance vulnerabilities. (2022 rank: 1)

3. **Data protection.**
   There are several issues wrapped up in data protection, ranging from cyber security attacks to compliance requirements and user access. (2022 rank: 4)

4. **Compliance status.**
   With multiple data locations, remote users and multi-country, multi-industry regulatory environments, it can be a challenge for businesses to truly understand their compliance status, let alone have good visibility into its current state. (2022 rank: 3)

5. **eDiscovery.**
   With digital being the default form for information and documents, eDiscovery is an important consideration for many companies to support requirements such as freedom of information requests, litigation, or government investigations. It is also increasingly difficult in a world of remote working and mobile devices where communication channels incorporate historical sources such as email and office productivity applications as well as 'newer' channels such as social media platforms, collaboration tools such as Slack, Microsoft Teams and even AI-driven conversation bots. (2022 rank: 5)

We have tracked the common data management challenges since the first edition of the report and whilst the order of the challenges may change, the broad issues have remained very similar over time.

It is interesting to note however that in 2023, sitting just outside this top 5 list, are 3 factors that have risen considerably in prominence since 2020, namely:

- **Managing data loss**
- **Preventing data leakage**
- **Managing dark data**

All 3 have doubled in importance as significant operational management challenges between 2022 and 2023 (admittedly from relatively low bases), and we would not be surprised if one or all of these issues form part of next year's top 5.

Data Management Challenge Priority	2021	2022	2023
1	Storage optimisation	Classification	Storage optimisation
2	Classification	Storage optimisation	Classification
3	Protection	Compliance	Protection
4	eDiscovery	Protection	Compliance
5	Compliance	eDiscovery	eDiscovery

"For us, we know we're going to face some issues (with multi-cloud infrastructure), especially with data migration and possible sovereignty concerns. We're looking at trying to build some form of cross-cloud management platform to mitigate against these."

Compliance Manager, Professional Services Company, APJ

In our 2nd edition we introduced research into the top operational challenges businesses faced with data. We continue this focus for 2023 and it is interesting to see the increase in prominence of problems with unstructured data as well as the lack of standardised data management tools and native cloud management tools tied to specific cloud platforms.

Ranking	2022	2023
1	Poor quality data	Too many data sources
2	Too many data sources	Unstructured data
3	Incorporating digital and paper-based information	Poor quality data
4	Inability to share information and data	No standardised data management platform/tools (2022 rank: 9)
5	Unstructured data	Native cloud data management tools tied to specific cloud platform (2022 rank: 10)

The issues of no standardised data management platform and native cloud data management tools can be troubling for organisations, especially so in a multi-cloud or hybrid infrastructure environment, as they can increase the complexities of cyber responses and data management.

Our research revealed the top 5 challenges of using native data management tools as follows:

1. **In a data recovery situation, cross-cloud solution incident response teams have disparate skills sets.**
2. **Additional complexity of managing solutions from multiple vendors.**
3. **Lack of consistent data protection policies across multi-cloud and hybrid environments.**
4. **Limited visibility across disparate platforms and cloud providers creates gaps in data management and protection.**
5. **Reduced efficiencies resulting from poor storage and data lifecycle management.**

The Commvault Perspective

The importance of classification and storage optimisation amongst the top 5 data management priorities is no surprise and reflects the ongoing desire of organisations to both drive value from, and reduce costs by, optimisation activities. Today, data management is about understanding the data and creating value and insights from it, rather than simply implementing storage, recovery, and backup solutions. It is clear that a number of risks to organisations can be caused by multi-generational data sprawl, ranging from data fragmentation, degradation of automation and process efficiencies, and as an increased surface for cyber attacks.

Companies that continue to maintain the status quo with current backup and data management tools and then accelerate their scripting and build activities will not close the gap between the increasing data sprawl and their business goals. Nor will adding additional point solutions to manage the sprawl, as this simply introduces greater data fragmentation and a higher risk exposure.

Using the cloud to manage data

In 2022 we noted *"Whilst the lift and shift to cloud infrastructure (IaaS) supports digital transformation, for many companies it no longer constitutes it. For those looking at drawing greater benefits from their data and getting it business ready, the next wave of cloud activity incorporates a focus on modernising data management capabilities to ensure organisations are not restricted by a sub-optimal data environment."*

This comment continues to hold true for 2023 with 76% of survey respondents either using cloud data management services or intending to deploy within the next 12 months.

Our respondents identified a range of benefits of cloud data management services compared to traditional approaches and we have noted their top 5 as follows:

1. **Automated backup**
2. **Easier data recovery**
3. **Automated updates to platforms and tools**
4. **Improved data access and governance compared to on-premises options**
5. **Improved security posture compared to on-premises options**

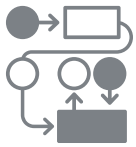
The table summarises the change in the top 5 derived benefits between 2022 and 2023:

	2022	2023
1	Improved data quality due to removal of data silos compared to on-premises	Automatic backup
2	Automatic backup	Easier data recovery
3	Easier data recovery	Automated updates to platforms and tools
4	Automated updates to platforms and tools	Improved data access and governance compared to on-premises
5	Improved data access and governance	Improved security compared to on-premises

"Our current approach is to try and use each cloud's specific data management tools as we're a little locked-in to them. The individual performance is pretty solid and we're happy with them each on a stand-alone basis... wrangling them all together for a consistent, seamless view is proving to be a little more difficult than we expected."

– IT Director, Retail Group, Australia

Data management regulations, roles, and responsibilities



Key findings

1. **Annual data growth rates have slowed, down from 40% in 2020 to 33% in 2023 with unstructured data constituting the largest component.**
2. **62% of all respondents are using multi-cloud or hybrid infrastructure to support their data estates.**
3. **Usage of cloud services for data management is high, and organisations need to be aware of the limitations of cloud-native tools tied to specific clouds.**

An average of 67% of organisations (68% in Australia, 64% in New Zealand) told us that they pursue a 'data driven' business strategy, a decrease of 11% from 2022. Whilst the percentage of organisations following a data driven approach is lower compared to 2022, the benefits are clear with companies citing a number of positives including:

1. **Using data to refine strategic focus and improve execution on decisions and initiatives.**
2. **Improved education of employees on how to access and use data to support decision making securely and appropriately.**
3. **Incorporating of metrics to quantify the success of data driven projects.**

Businesses in ANZ told us they expect 2023 to be a challenging year when it comes to legislative and regulatory changes impacting their data management operations. 72% of respondents are preparing for changes in the next 12 months and 58% are already subject to data sovereignty regulations.

These changes are wide-ranging and are expected to impact in multiple ways, of which the top 5 are:

1. **Requiring a change and improvement in data security capabilities.**
2. **Planning for monetary or other penalties if there is a data breach.**
3. **Increased complexity in data management including changes to what data is gathered and which parties have access.**
4. **Uplifting in-house data management skills amongst employees and/or turning to third party managed service providers to support in-house operations.**
5. **A need to provide access to data for government agencies.**

"We're taking a deeper look at our data management capabilities than we have in the past. It's a mix of cost optimisation as well as making sure we're across our compliance requirements with multiple regulations we have to deal with."

– CIO National Financial Services Group, Australia

Clear responsibility for data management and protection has always been important and with the expected impact of additional changes, even more so in 2023.

We asked ANZ respondents which role holds responsibility for data management and protection, and they told us:

- **IT Directors: 22%**
- **CIOs: 21%**
- **CEOs: 10%**
- **CDOs: 9%**
- **CFO: 8%**
- **CISO: 5%**

However, 27% of organisations are operating without a clear, single point of responsibility: 18% of companies stated that it is 'blended across multiple roles' and another 9% stated it was unclear within their organisation. This percentage was higher in New Zealand (30%) than Australia (23%).

Whilst this lack of singular responsibility may increase the potential risk exposure in those organisations, the risk is mitigated given that 89% of all respondents have a data management plan (DMP) either already in place or in development.

The top 5 areas included within a DMP include:

1. **A data recovery plan;**
2. **Documentation and descriptions of all data held including types, sources, and formats of the data;**
3. **How and where data is stored and secured;**
4. **Provisions for data protection and privacy; and**
5. **Data controls including user access, sharing, dissemination and re-use.**

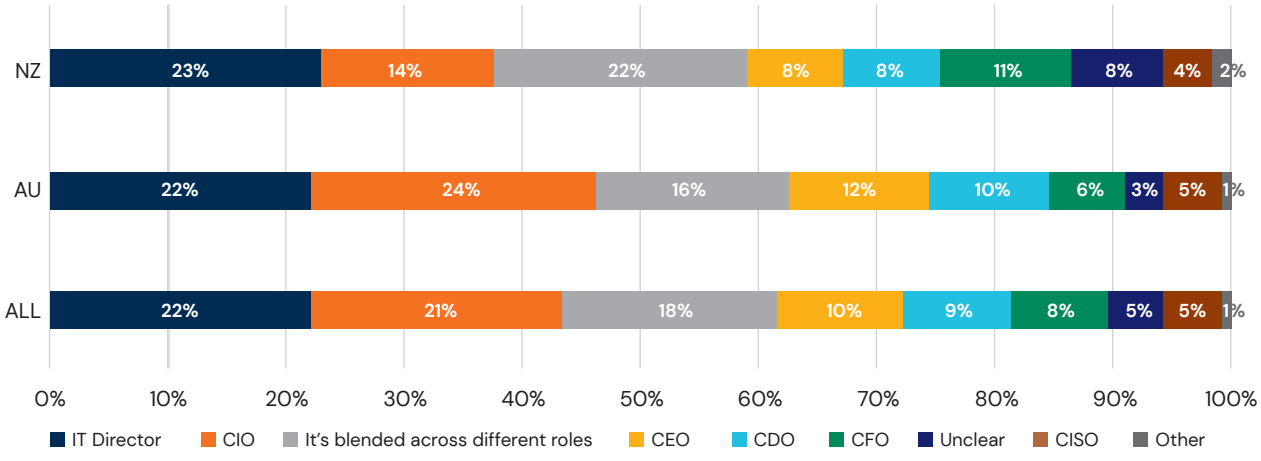
The Commvault Perspective

A multi-infrastructure data estate is the default approach for the majority of companies and, as organisational compliance demands continue to grow, it is increasingly difficult to build an effective compliance framework without creating a platform that spans multiple infrastructure types.

Businesses should consider data management from an organisation-wide perspective and not something that falls to a single department. Disparate data infrastructure environments can potentially make it harder to ensure regulatory oversite as well as rendering cyber security policies ineffectual and difficult to administer.

It is therefore critical to use a management suite that provides comprehensive services spanning data backup, disaster recovery, archiving and cloud management that simplifies and automates the data management process.

Which role in your company holds management and operational responsibility for data management and protection?



Data breaches, outages, and recovery

Key findings

1. **The percentage of companies experiencing a data breach or loss due to a cyber attack has significantly reduced from 79% in 2021 to 35% in 2023.**
2. **Of those that lost data, those that could recover 100% have reduced. Only 40% of companies breached managed to recover 100% of their data in 2023, compared to 47% in 2021.**
3. **Attacks simultaneously targeting all data estates (production, secondary and backup) have increased since 2020, with 22% of companies reporting this was the approach taken with their most recently experienced attack in 2023.**
4. **Only 6% of companies were proactively alerted to an attack by their own internal systems and tools.**

Cyber Attacks, Data Losses and Data Estates Targeted

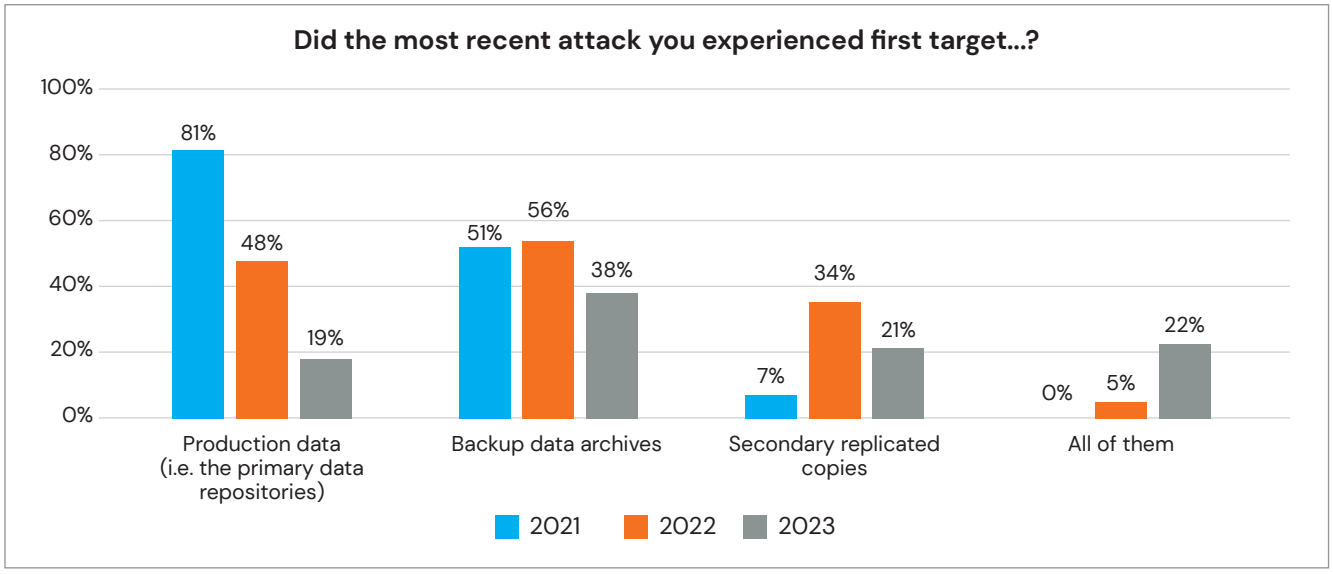
Any analysis of data management issues demands a discussion around the cyber security environment, threat vectors, data loss, and time to recover.

72% of respondents indicated that they were subject to a cyber attack and whilst cyber attacks have become daily occurrences for many organisations, this year's data revealed one positive fact – of those companies attacked, an average of 35% suffered a data breach or loss (down from 79% in 2021 and 67% in 2022).

Australian companies saw the biggest drop in data breach or losses between 2021 (83%) and 2023 (36%), with New Zealand companies citing 67% in 2021 and 32% in 2023.

There is growing awareness amongst ANZ organisations that threat actors are increasingly targeting more than just primary production data with ransomware and other cyber security attacks.

In previous years our research showed that companies were experiencing both backup and secondary data sources being targeted and a growing number also reported a 'nuclear option' of everything being simultaneously attacked. The 2023 data clearly shows the continuation of this trend as can be seen in the chart below.



"Trying to recover the data is always a pain. This is the second time we've been breached and had to recover... we learnt from the first time. That time we lost our backup data as well and it took over a month to fully recover. We took steps after that to make sure we had strengthened our protection of both secondary and backup sources."

- CISO Health Services Group, Oceania & ASEAN

For this year's research we wanted to understand if organisations were aware of this issue and recognised the problems it could cause. The answer is 'yes, mostly':

- **45% stated secondary data sets were targeted at a similar level to primary data (43% in AU, 48% in NZ);**
- **26% stated secondary data sets were targeted more than primary data (28% in AU, 22% in NZ);**
- **22% stated it is not an issue (22% in both AU and NZ); and**
- **7% hadn't considered it (7% in AU, 8% in NZ).**

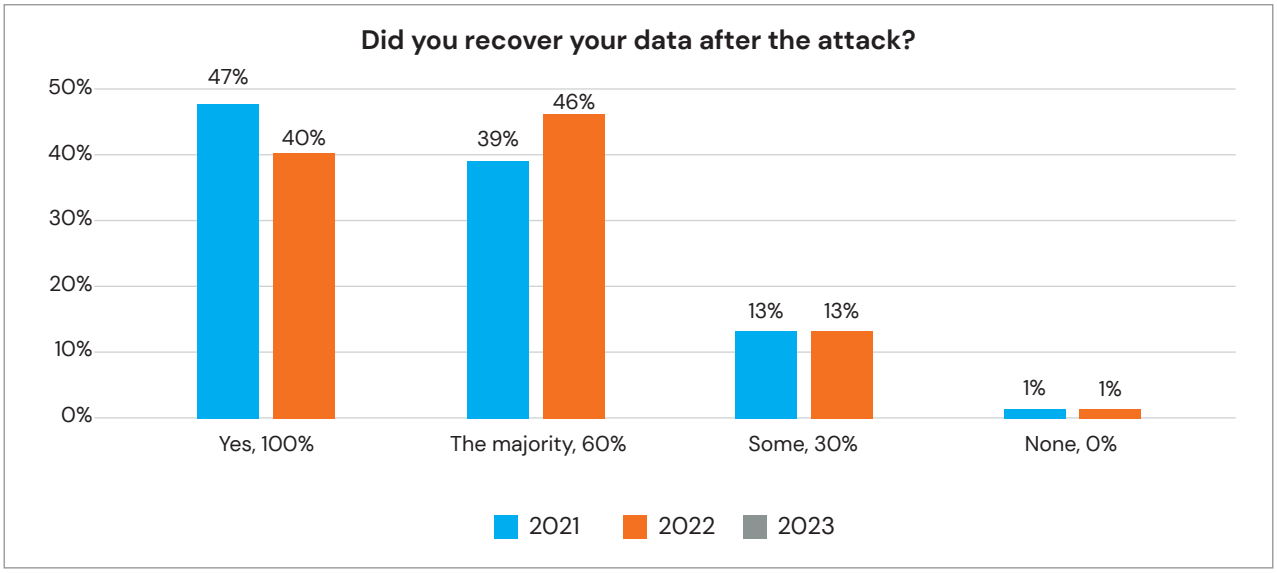
Delving a little more deeply into the research we found that for those stating it was 'not an issue', in Australia 24% had experienced attacks on their secondary data sets with 8% in New Zealand experiencing the same.

For those organisations that 'hadn't considered' the issue, 23% in Australia and 28% in New Zealand had experienced attacks on their secondary data sets.

Data Recovery Rates and Time to Restore

With attacks increasingly focusing on both primary and secondary data sets, the disruptive intent is clear, and its effectiveness (for threat actors) can be seen in the data detailing recovery rates.

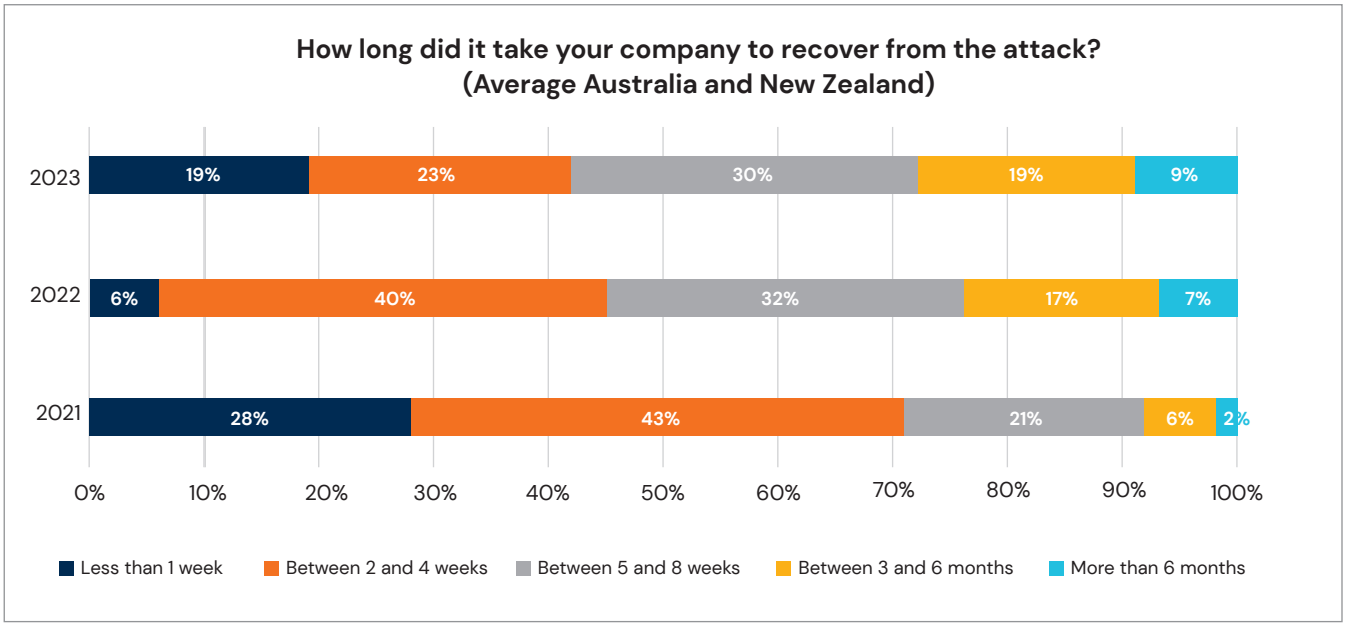
Comparing data from 2021 to 2023 shows that organisations are experiencing a fall in 100% recovery of lost or breached data from 47% to 40%.

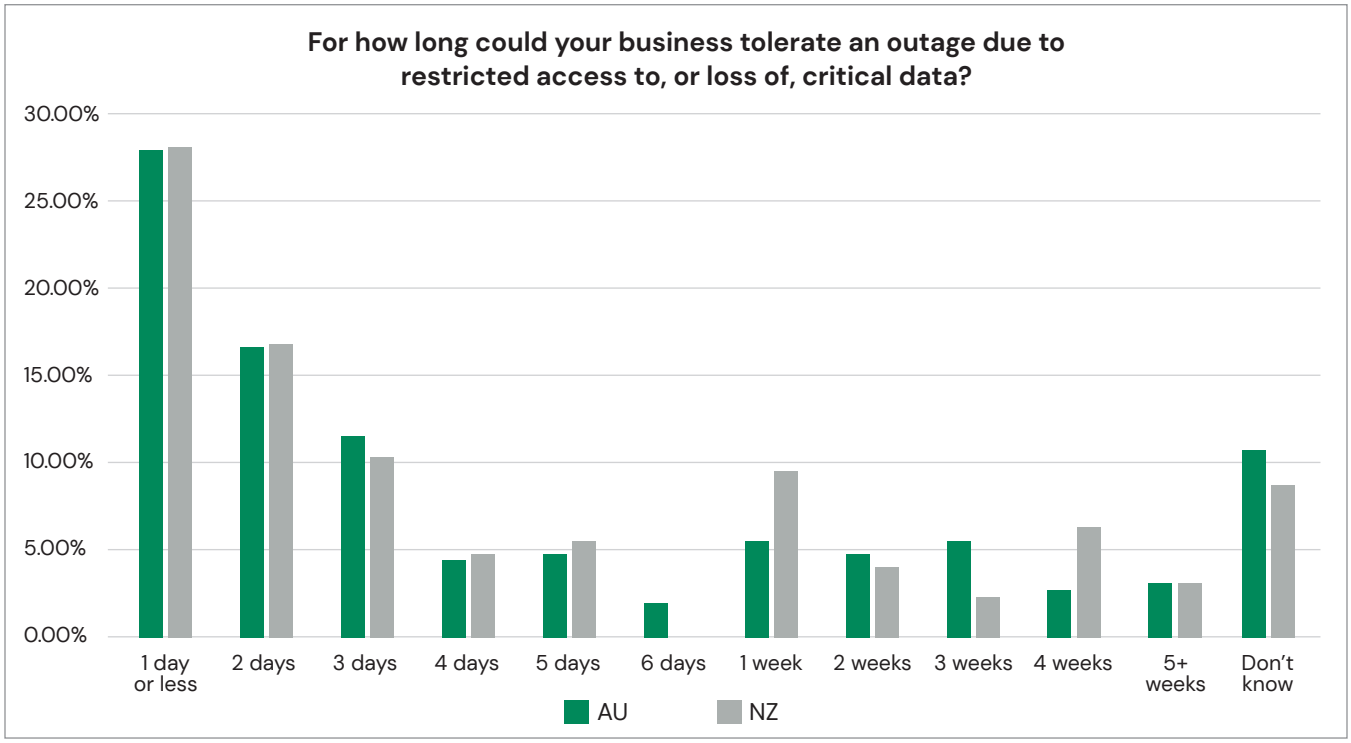


So, organisations are suffering less data losses and breaches from cyber attacks but recovering less when breached. What about time to recover? It's getting longer.

In 2021, 28% of companies recovered within 1 week and 71% within 4 weeks. In 2023, those percentages fell to 19% and 23% respectively.

The increase in recovery times contrasts very starkly with the tolerance businesses have for an outage that causes a loss of access to, or loss of, critical data: 65% of companies (the same in both Australia and New Zealand) state their operation could not tolerate a data outage for longer than 5 days.





Of course, it's not just the perceived 'tolerance' of the business that is the issue, the consequences of a data breach or loss to companies is significant, ranging from reputational damage, legal action, to potential loss of employment for those involved.

Businesses told us their top 5 negative impacts from data losses or breaches are as follows:

Ranking	2022	2023
1	Not compliant	Reputational damage
2	Reputational damage	Unable to service customers
3	Damage to IT's reputation	Revenue loss
4	Revenue loss	Business-wide disruption
5	Job security	Legal action

The importance of reputational damage and inability to service customers is further accentuated when considering how organisations discovered they had been breached and lost data. In 2022, only 3 companies (less than 1% of all respondents) stated they had first discovered the attack when their security systems and tools alerted them to an attack in progress. In 2023, that number had improved, but only marginally to 6% of the total (or 23 companies).

Of the top 5 ways companies discovered their misfortune, all are reactionary and after the event:

1. **When informed by a third-party security provider, typically a managed security provider (MSP), after the attack was underway or over.**
2. **When unable to access internal data or systems.**
3. **When confidential information or data was found in the public domain or dark web.**
4. **When contacted by the threat actors.**
5. **When approached by a news or media organisation or journalist.**

The Commvault Perspective

Ransomware and other types of cyber security attacks are here to stay. It is obvious there is a clear trend of threat actors primarily focusing on encrypting all critical business data (across production, secondary and backup data estates) and then attempting to extort ransom payments.

In response to this we are seeing large numbers of companies looking to leverage backup solutions to protect their data and mission critical business operations. These organisations now have the requisite tools to recover encrypted data and get their business back online.

Understanding this, threat actors continue to evolve the sophistication of their approaches and are targeting organisations in new and unique ways looking to create a triple data extortion threat of leakage, exfiltration and theft. In certain instances, these attacks no longer bother to encrypt the targeted companies' data (and subsequent request for a decryption ransom payment) and move directly to the increased threat of leaking the data to the public domain, or in some instances, even to competitors.

It's clear that whilst conventional backups provide the ability to recover data post-encryption, they often come into play when it's too late, after critical data has already been exploited. To comprehensively secure data from these threats, we must rethink data protection to start before your company is compromised, not just at the point of recovery.

In Closing

In this third edition we have seen the continued evolution of key trends namely:

1. **A slowing in the rate of yearly data growth;**
2. **The ongoing use of multi-infrastructure to support data estates;**
3. **The persistence of unstructured and dark data; and**
4. **The ever-present threat of cyber security attacks.**

Importantly we have also noted the increased focus on a more considered evaluation of stored data, its strategic value, and the level of risk exposed by continuing to hold 'no-value' data, especially in the light of a data breach or loss. We expect this focus, as well as a possible continued slowing of data growth, to continue throughout 2023 and 2024, especially as companies continue to push hard with cost reduction activities through improved data optimisation.

How Can Commvault Help?

There are a myriad of data management challenges and complexities that can disrupt or destroy the data on which your company runs. Commvault can help you with these challenges by providing a comprehensive, trusted suite of data management and protection solutions that allow you to manage, protect and use your data in a consistent and efficient manner including:

1. **Data backup and recovery for fast, reliable, and efficient data protection and disaster recovery.**
2. **Improved data security, protecting against cyber attack, unauthorised access, and data breaches.**
3. **Enhanced, effective cloud data management that allows you to leverage the benefits of cloud(s) and ensure strong data management, protection, and governance.**
4. **Simplified data archiving that supports classification and optimisation (and subsequent lower costs).**
5. **Improved data utilisation that helps you access and gain insights from your data to support informed business decisions.**

Where to start?

A Commvault Recovery Readiness Assessment is available to help determine your ability to quickly recover data and systems across your environment. Data protection experts can help identify and propose a path forward by providing an executive scorecard as a measure of your ability to respond to a partial or mass recovery scenario. This is the ideal starting point for quantifying response times for a return to normal business operations.

In the event of a disaster or ransomware attack, you can not afford to lose valuable time trying to formulate a plan or inefficient processes. Commvault can provide the services to help you prepare a readiness plan so you are recovery ready.

DATA SOURCES

The data and commentary presented in this report is drawn from a blended research approach comprising a market research survey supplemented with telephone interviews with companies in Australia and New Zealand and senior Commvault executives. The survey was conducted in January 2023 with a sample size of 376 companies of more than 100 employees in Australia and 50 employees in New Zealand.

ABOUT TECH RESEARCH ASIA (TRA)

TRA is a technology 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 provide 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. TRA also publishes the open and online journal, TQ. To learn more, visit www.techresearch.asia.

ABOUT COMMVAULT

Commvault is a global leader in data management. Our Intelligent Data Services help your organisation do amazing things with your data by transforming how you protect, store, and use it. We provide a simple and unified Data Management Platform that spans all your data – regardless of where it lives (on-premises, hybrid, or multi-cloud) or how it's structured (legacy applications, databases, VMs, or containers). Commvault solutions are available through any combination of software subscriptions, integrated appliances, partner-managed or Software-as-a-Service via our Metallic portfolio. Throughout 25 years, more than 100,000 customers have relied on Commvault to keep their data secure, assessable, and ready to drive business growth. Learn more at www.Commvault.com.