



State of Cloud, Edge, and Security in Australia 2023-24

How Australian executives are securely leveraging cloud and edge for meaningful business change



Contents

| | |
|---|----|
| 1.0 Summary | 3 |
| 2.0 Key Statistics | 5 |
| 3.0 State of Cloud – Australia in 2023-24 | 12 |
| 4.0 On the Edge – Australian firms actively explore the possibilities | 23 |
| 5.0 Securing Australia – Cyber Security Challenges and Opportunities | 28 |
| 6.0 A Path Forward – Recommendations | 34 |
| 7.0 Appendix | 37 |

1.0 Summary



Summary

Telstra has collaborated with Omdia for the third consecutive year to conduct an in-depth study and compile the insights. This annual "State of Cloud, Edge, and Security" research sheds light on how prominent Australian business, enterprise, and government entities leverage cloud, edge, and cyber security to drive digital transformation.

This year's research indicates that most cloud investments aim to promote digitisation, modernise applications, and improve cyber security. However, benefits are often elusive; while pursuing innovation and modernisation, Australian organisations often settle for Total Cost of Ownership (TCO) benefits. Security, data governance, and customer experience remain significant challenges.

Standout revelations include both a surge in edge computing adoption and the critical role of a well-architected and managed network. Our research found that 69% of Australian leaders deem network expertise pivotal when selecting their managed cloud service provider. Further, as security incidents and their detrimental impacts rise, the potential of SD-WAN to bolster cloud migrations and ongoing security concerns is becoming more evident.

The paper concludes with recommendations to redefine the business case behind cloud migrations, pursue even greater cyber security and network resiliency, and leverage the right partners to overcome complexity, accelerate time to value, and reduce technology risk.

2.0 Key Statistics

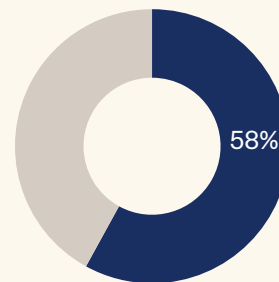


Cloud – Powering transformation, modernisation, and security investments

Cloud Migration in Australia – Benefits remain elusive.

- Nearly 60% of Australian organisations report having 'completed' a recent major transformation project where hybrid or multi-cloud capabilities were essential.
- Of those, roughly half were to support a company's broader digitisation journey, drive application modernisation, and uplift cyber security.¹
- The most progressed transformation areas are supply chain and logistics, employee experience, and sales and marketing.
- As a result, public cloud and SaaS adoption jumped 10% over the prior year's survey, now supporting 43% of critical applications in Australia.
- Hybrid cloud remains the dominant approach in Australia, supporting 57% of critical workloads.
- In more than 46% of cases, the CEO, CIO, or CTO remain key decision-makers in choosing the service provider. Notably, the risk office (e.g., legal and security officers) has overtaken procurement and finance as key influencers in the choice of provider across cloud, security, or edge.

Australian businesses that completed major digital advancement initiatives



Note: n=170

©2023 Omdia

Most progressed areas of transformation



Sales & Marketing

69%
Completed



Employee Experience

58%
Completed



Supply Chain and Logistics

53%
Completed

Benefits are emerging but non-uniform and elusive.

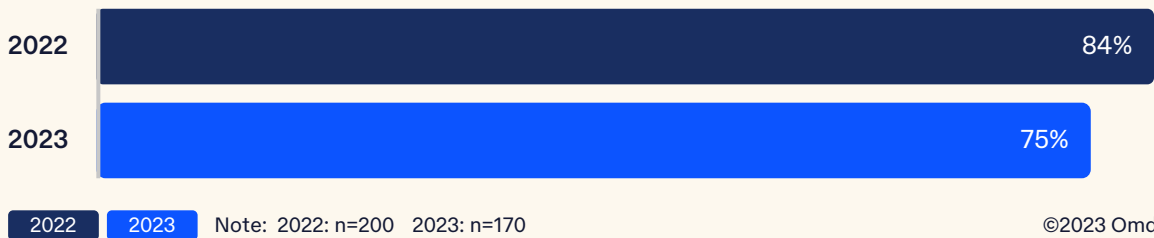
- While an impressive 75% of recent mission-critical cloud migrations met or exceeded their business case, this success rate has seen a dip from last year's 84%. This decline can be attributed to the intricate challenges posed by hybrid cloud complexity, a shortage of essential skills, and persistent security threats.
- Total Cost of Ownership (TCO) reductions were the most common measure to appropriate investment value, but effectively quantifying the broader benefits of transformation proved more elusive.
- A mere 55% of the latest major cloud migrations successfully met or surpassed their business cases, particularly in driving broader digital transformation ambitions. Australian executives are still somewhat dissatisfied with their latest cloud migration project. Only 22% of organisations are 'delighted'; most are only partially satisfied.

¹ In this study, hybrid cloud is any combination of interconnected internal (private) and external (public) cloud services from one or more providers in the delivery of an organisations business applications, workloads, or functions. By contrast, multi-cloud refers to using two or more public clouds that may be connected or independent.

Unpacking the current and emerging challenges in cloud migration.

- Security, data, and customer experience challenges are cited as fundamental barriers to the successful realisation of digital transformation by nearly 25% of leaders.
- 40% of Australian organisations are now 'well prepared' for cloud migration challenges, down marginally from 41% in 2022.
- Over 30% of firms cite a lack of cloud strategy, skills, and security as the top three concerns when modernising in the cloud.
- In the foreseeable future, a significant 32% of firms foresee the Environmental, Social and Governance (ESG) movement as the primary challenge to sustaining ongoing digital transformation initiatives. On average, only 11% of firms, have put in place strategies utilising technology-driven transformation to advance their ESG objectives.

Mission-critical cloud migrations that met their business case



The primacy of a well-designed and managed network remains.

- Half of the surveyed firms (50%) consider Managed SD-WAN, while 49% rely on Ethernet VPN, as indispensable for essential backhaul connectivity in their hybrid cloud setups.
- Consistent with prior years, most (69%) Australian leaders insist that network expertise remains a paramount decision factor in choosing their managed cloud service provider.
- As security incident rates rise, SD-WAN underpins future cloud migrations, and security concerns persist, a rapid adoption of Secure Access Service Edge (SASE) is anticipated.
- Similar to other advanced nations, the concept of a sovereign cloud has gained paramount importance for a majority of firms in Australia, especially for government agencies and departments. It is now considered indispensable in choosing a hybrid cloud provider.

For majority of Australian leaders, network expertise is paramount in managed cloud service provider choice



Note: n=170

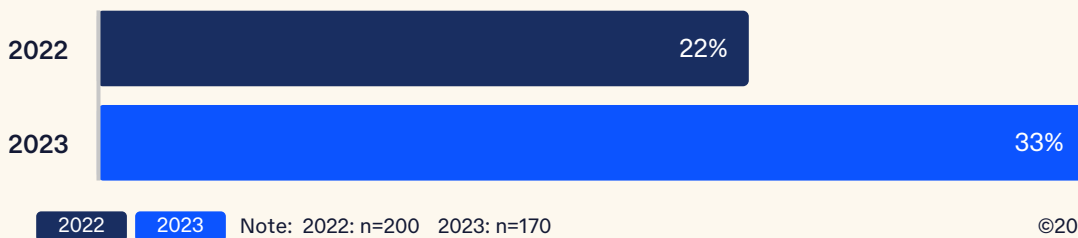
©2023 Omdia

Edge – Australian firms actively explore the possibilities

Edge deployments and curiosity among Australian executives are rapidly increasing.

- Edge deployments have increased since the prior survey. Around 33% of firms run edge computing, up from 22% last year.
- The top five mainstay deployments are IoT, business intelligence (BI), video streaming and analytics, custom applications, and high-performance computing at remote and branch sites.
- Many novel use cases are emerging, and local executives unanimously showed interest in further exploring edge solutions in future technology investments.
- Over a third of Australian enterprises expect to deploy additional edge solutions in the next 18 months. Many executives are currently considering or experimenting with edge POCs ahead of planned deployments at scale.
- Edge is gaining importance as data volumes are growing and enterprises aim to minimise network costs by processing data closer to users. It is also critical for low latency, e.g., for worker safety that depends on milliseconds.
- Decision-makers are increasingly understanding the benefits of edge as the technology is going mainstream, minimising some of the early fears regarding security and complexity.

Edge deployments have increased since the prior survey



The top five mainstay edge deployments



61%
IoT



59%
Business
Intelligence



49%
Video Streaming
and Intelligence



38%
Custom Apps

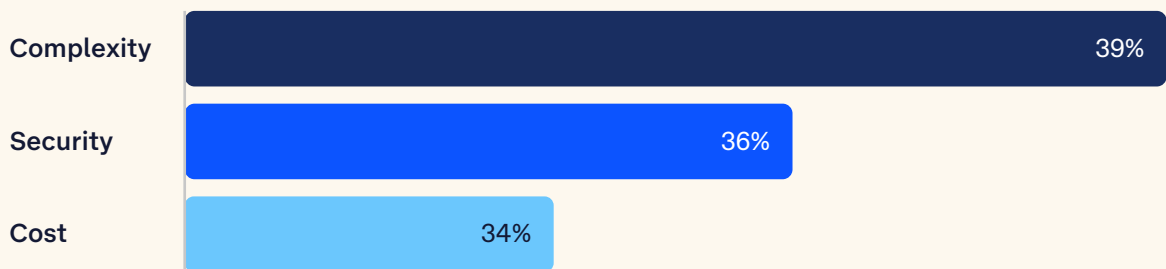


34%
High-Performance
Computing

Edge adoption is burgeoning, despite challenges stemming from its flexibility.²

- The inherent flexibility of edge brings concomitant complexity for many executives. In this year's research, 39% of organisations cite 'complexity' as the biggest edge adoption constraint, followed by 'security' at 36% and 'cost' at 34%. These results suggest that many Australian executives do not yet fully understand the benefits and value of the edge and (often incorrectly) perceive it to be less secure.
- The flexibility of edge compute capabilities with other emerging tech introduces complexity as edge innovative and successful solutions tend to integrate with other technologies, including 4G/5G, Fixed Wireless Access (FWA), Internet of Things (IoT), and artificial intelligence (AI).
- As a result, most firms presently leverage edge for operational goals (33%) compared to only 12% for innovation. However, in nearly every interview, innovation is the kernel of most new deployments.
- Enterprise IT has transformed on Cloud. However, Operational IT is not as progressed but can accelerate transformation of industrial automation using Edge.
- Consequently, Edge will become vital to maintaining a competitive advantage as part of enterprises' future investment roadmap. Thirty-three percent of Australian enterprises expect to deploy additional edge solutions in the next 18 months.

Factors hindering edge adoption



Note: n=170

©2023 Omdia

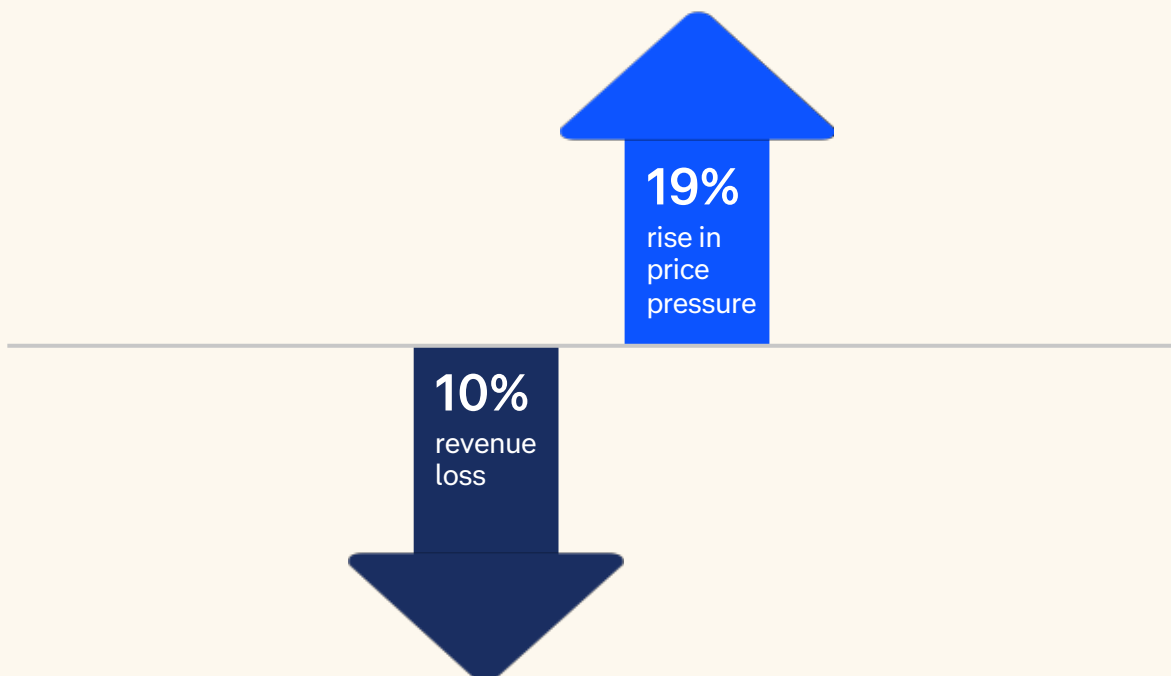
² Edge computing is a distributed computing paradigm that brings application data, computational and storage capacity closer to the data sources than centralised private and public cloud computing platforms provide. Edge computing can be deployed for local data processing (site edge) or as a gateway to cloud computing and data centre resources (far/near edge).

The ongoing significance of Cyber Security

Attacks have increased, with adverse impacts.

- Concerningly, 61% of Australian organisations have experienced a significant increase in overall security incidents in the last 12 months, up from 57% last year. Moreover, 23% have experienced substantial growth in serious security issues in the past 12 months; notable increases have punctured endpoints, IoT and public cloud bastions.
- Further, over a third of Australian organisations have grappled detrimental consequences following recent cyber incidents or breaches. Fifty-four percent of Australian firms report losing revenue, 52% suffered reputational damage and 46% operational downtime. This could be attributed to various factors, such as disruptions in business operations, potential fines or penalties, or the costs associated with recovering from the cyber incident. A little over half of the organisations surveyed have faced negative publicity, loss of customer trust, or a damaged brand image due to the cyber incident. The consequences of operational downtime could mean including delays in delivering products or services, missed business opportunities, and increased costs associated with recovery efforts.
- These statistics collectively demonstrate the substantial impact that cyber incidents can have on businesses, affecting their financial stability, reputation, and day-to-day operations.
- Most alarming, the research indicates Australian firms lost, on average, over 10% of revenue from the most recent cyber breach. The impact was also a 19% rise in price pressure passed onto customers or deteriorating margins.

Adverse impacts of cyber security breaches



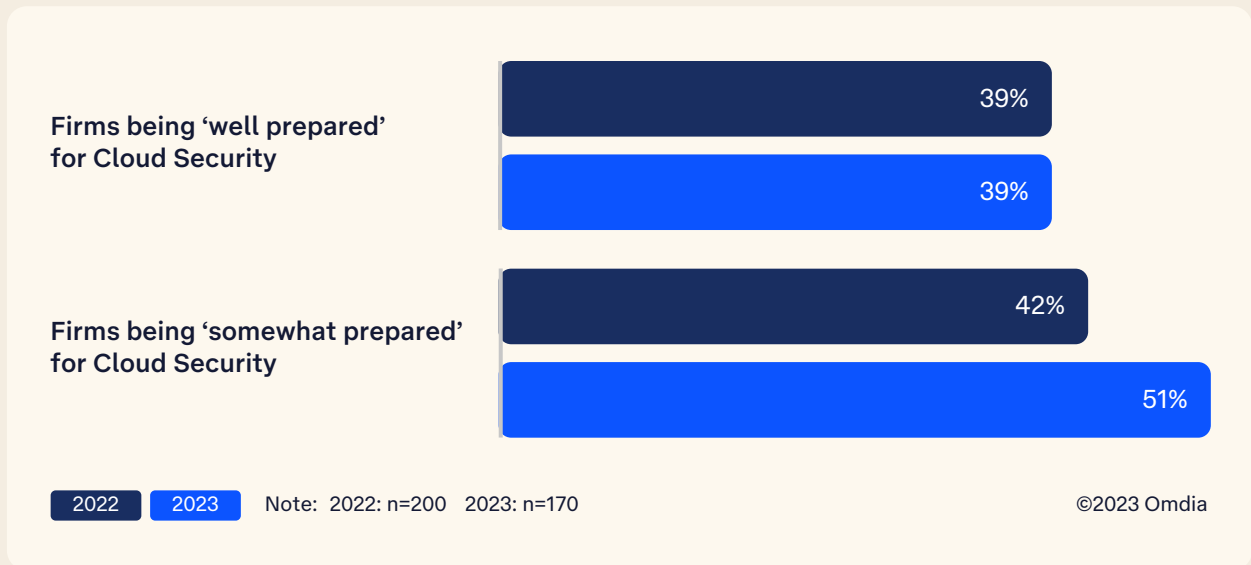
Note: n=170

©2023 Omdia



Peering ahead, cloud security preparedness stalls, and outsourcing grows.

- Progressing into 2024, only 39% of Australian firms are 'well prepared' for cloud security, unchanged from last year's survey.
- Redoubtable challenges loom for many, as the average percentage of leaders being 'somewhat prepared' has fallen to 42%, down from 51% in last year's survey.
- Wavering preparation is often rooted in a lack of preparedness in securing mission-critical cloud; over a third of firms are 'not at all prepared' for cloud integration with existing security (in-house, SIEM, SOC), 21% in change management, and 18% in leveraging technologies and platforms (e.g., SASE).
- With growing cyber threats from criminals and rogue states, skills shortages in threat detection, response, and recovery across complex IT and slowly growing budgets, security leaders are resolute and intend to focus heavily on security strategy and proactive elements.
- An increased demand for security consulting and professional services to tackle challenges amid a competitive labour market is expected.



3.0 State of Cloud – Australia in 2023-24



Cloud Migration in Australia – Benefits remain elusive

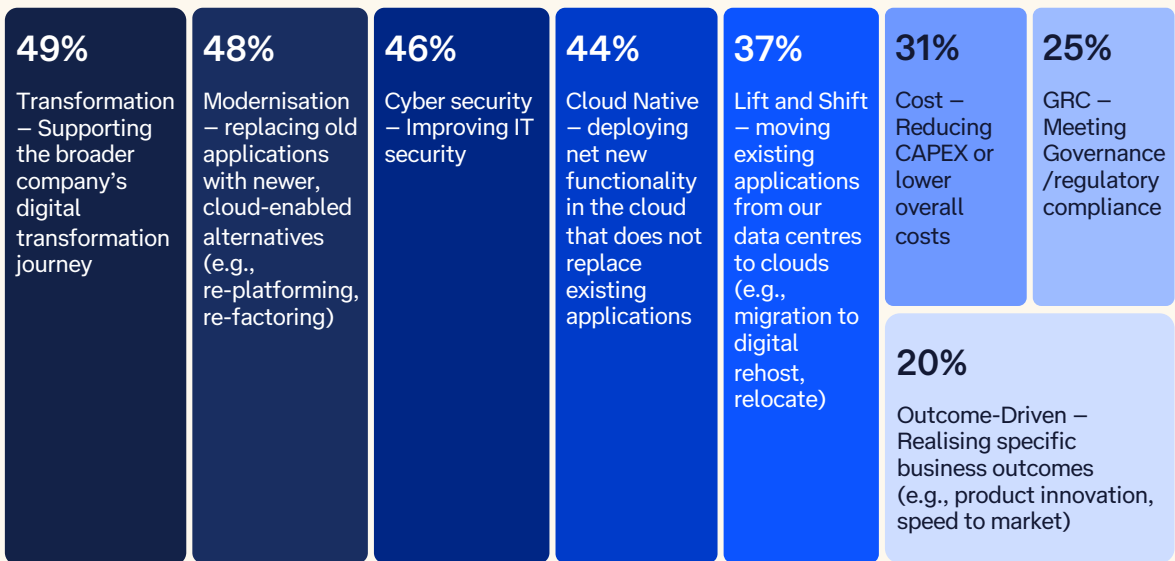
Most firms want modernisation and transformation but settle for cost reductions.

In the pursuit of progress, many companies initially aim for modernisation and transformation but often settle for mere cost-cutting measures. However, this year's research sheds light on a crucial shift: substantial cloud investments play a pivotal role in driving a company's broader digitisation journey, steering application modernisation, and fortifying cyber security (refer to Figure 1).

Lift and shift remain essential and present a significant juncture – it's usually tactical, triggered by an end-of-life migration, but often triggers a rethink of the more expansive cloud and application environment. Visionary leaders adeptly leverage this tactic to catalyse broader transformational initiatives.

It's also important to note that the top four investment drivers for the hybrid cloud are tightly clustered, proving problematic for decision-makers accountable for explaining and measuring realised business benefits.

Figure 1 – What's driving your most significant investments involving the cloud?
(Percentage of respondents)



Note: n=170

©2023 Omdia

Critical cloud migration shortfalls

On average, 75% of mission-critical cloud migrations 'met' or 'exceeded' business cases, but results are uneven and down from last year.

The good news first; in the past year, most Australian organisations met or exceeded business cases in TCO, IT agility, and risk reduction for significant migrations. (Figure 2)

Unfortunately, however, this represents a notable drop from 2022, when an impressive 84% of firms achieved or surpassed their business case objectives. While TCO reductions proved relatively straightforward to quantify in 86% of cases, executives grapple with effectively measuring and assessing the benefits of more intangible and elusive goals. Economic headwinds will fuel continued requirements for cloud migration to deliver TCO reductions and efficiency improvements.

Despite firms primarily targeting 'transformation', 'modernisation' and 'cyber security' benefits, the largest YoY drop in realised benefits stemmed when comparing 2022 to 2023 data, were shortfalls against the business case in security and compliance, innovation (direct contribution to agility including faster time to market), incremental revenues, and total cost benefit.

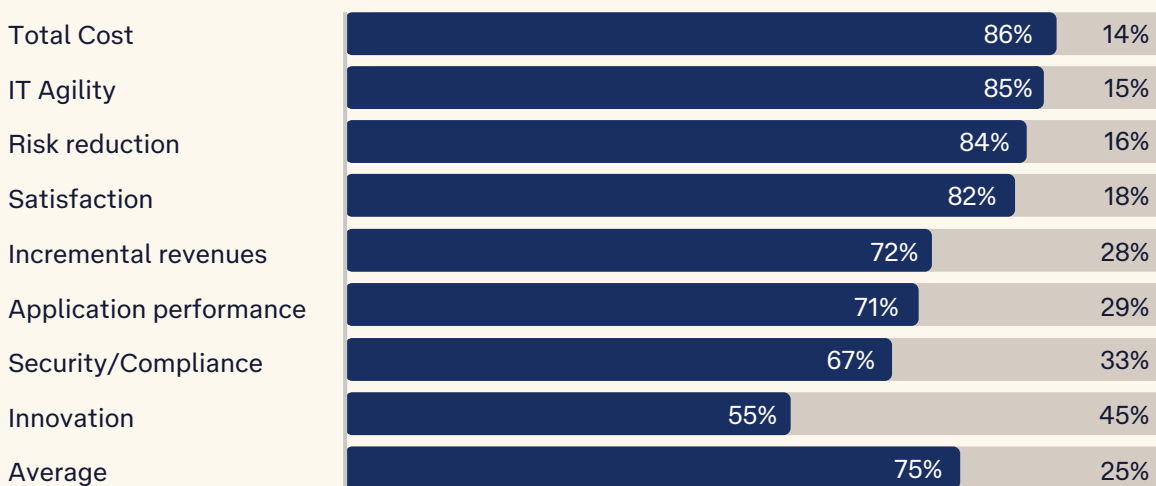
It is imperative that business leaders re-evaluate strategies, continue to allocate resources strategically, and ensure that cloud migration initiatives are not only meeting but surpassing their intended objectives. The time for action is now.

“ Digital transformation can mean many things. For us it’s changing the way we operate from how to ‘support the business’, to providing the ‘best platform for business innovation’ we can build.”

“ Examples like capturing rich data from IoT devices our SCADA, flowing through to ERP analytics, accessible to key users, scalable and accessible and virtualised to keep costs down aligning with major regulatory resets.”

CIO of a major Australian utility firm

Figure 2 – In the past 12 to 18 months, how well have mission-critical cloud migrations delivered against business case expectations? (Percentage of respondents)



Met or exceeded

Did not meet or don't track

Note: n=170

©2023 Omdia

Nearly 40% of Australian organisations have completed a major transformation project.

Fifty-eight percent of Australian businesses utilising cloud technology have successfully concluded significant hybrid cloud and cyber security transformation projects. The interviews with industry leaders further affirm substantial progress in achieving digital transformation through network evolution, including technologies like SD-WAN, edge computing, and IoT. The forefront of digital advancement lies in leveraging technology to enhance sales and marketing (69% have completed digitally enabled change initiatives), as well as improving employee experience, productivity, and tools (58%), along with optimising supply chain and logistics (53%).

Where the authority lies.

Understanding who's behind major investment decisions in selecting a strategic cloud, edge or security provider is essential.

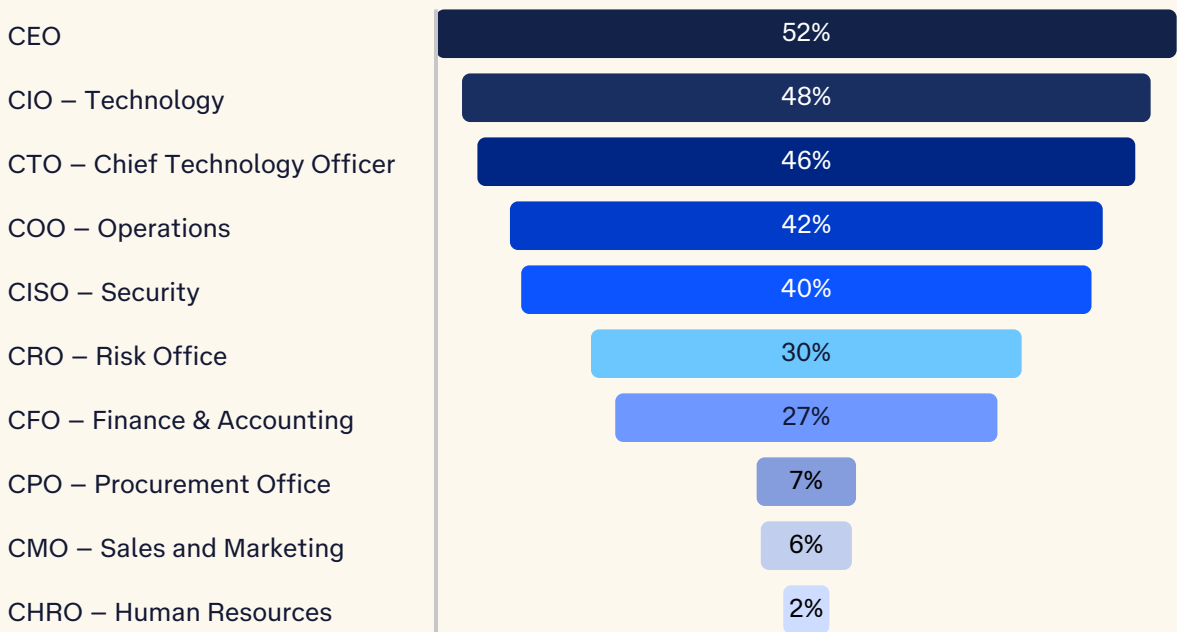
In more than 46% of cases, the CEO, CIO, and CTO remain key decision-makers in choosing the service provider. (Figure 3)

Notably, the risk office has overtaken procurement and finance as key influencers in the choice of provider across cloud, security, or edge. Nonetheless, the CFO and finance functions are often obligatory, demanding that business cases address cost-benefit requirements. For this reason, most projects' total cost is the default measure of success.

We foresee a return to more centralised decision-making, and the Line of Business impact over decision-making will wane toward 'influencer' rather than the final decision-maker.

Challenging macroeconomic conditions, including rising interest rates and synchronous effects of the cost of capital (ROIC), along with cloud sprawl, and migrating the remaining 'difficult' workloads will coalesce, bringing additional scrutiny to new business cases.

Figure 3 – Who are the top three decision makers or influencers in your organisation's strategic cloud, edge, or security provider choice? (Percentage of respondents)



Note: n=170

©2023 Omdia

Australian executives are still somewhat dissatisfied with their most recent cloud migration project.

Only 22% of firms are ‘absolutely delighted’ with their most recent major cloud project (Figure 4).

And while no respondents would consider past migrations a complete disaster; however, there is clear room for improvement.

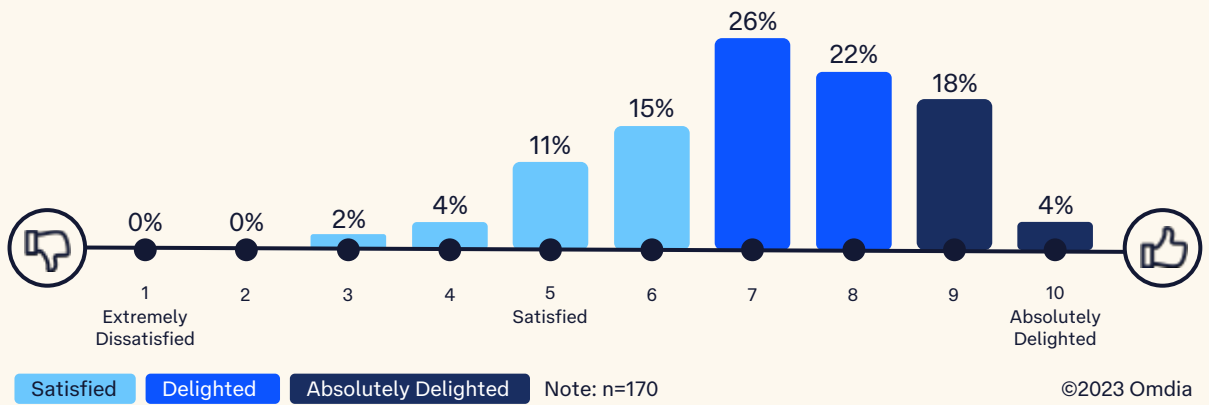
The satisfaction results reflect missed expectations against mixed business case results (e.g., shooting for innovation and revenue growth but settling for TCO reductions) and overcoming sizeable challenges that often only emerge after a project’s initiation.

On how to measure business benefits of cloud migration:

“ Our budget is more than just to modernise the applications. Whether it's business critical or not and regardless of any overlaps, we think about consolidation and rationalisation. ”

CTO of a major insurer

Figure 4 – How satisfied are you with your most recent / latest major cloud migration project?



Challenges mount in security, data, and customer experience.

To unpack the ambivalence, we asked firms to report on their biggest challenges in recent major digital change programs. Over a quarter of leaders indicate security, data, and customer experience are the most difficult. (Figure 5)

Figure 5 – What are the biggest challenges to realising success with digital transformation in your organisation?

| Challenge | Percentage of respondents |
|---|---------------------------|
| Security – Increased cyber security and digital risks | 26% |
| Data – Exploiting the value of data across the business | 25% |
| CX – Improving customer experience | 25% |
| Skills Gap – Attracting and retaining talented resources | 22% |
| Strategy – Articulating a clear digital strategy | 20% |
| Budget – Financial constraints from an economic slowdown | 20% |
| Legacy Systems – 'technology debt' | 18% |

Note: n=170

©2023 Omdia

Security and data governance issues run deep and are intertwined. Recent privacy breaches and cyber extortion raises the stakes for firms and governments of all sizes. Moving applications to public cloud or SaaS doesn't alleviate or isolate organisations responsibility for security. Firms must still ensure the underlying network, APIs, authentication other essential application layer security posture impacting processes, systems, and people.

Customer experience skills often map to data silos, complexity in application interoperability (including multiple APIs) and cultural barriers (not invented here syndrome).

Addressing skills gaps is a longstanding and pervasive issue. Expertise in data management, hybrid-cloud architecture, change management, cyber, and, increasingly, AI is often rare and/or expensive.

“ Around six years ago our integrator moved workloads to the public cloud, but it was poorly done. But I’m not going to blame the integrator, because back then, the frameworks that the cloud service provider offered were not that well architected. ”

So, this environment needed to be rebuilt as it's overly complex and complicated from a network perspective which actually makes it less secure. ”

Head of IT at a large Australian manufacturer

Environmental, Social and Governance (ESG) impacts loom.

Sustainability is a burgeoning topic, permeating from the boardroom to operations. Thirty-two percent of firms anticipate ESG will constitute the biggest challenge to continuing new digital change programs this year, elevating ESG above all other challenges alongside security and customer experience. (Figure 6)

Figure 6 – What are the biggest future challenges to realising success with digital transformation in your organisation? (Percentage of respondents, top five shown)

| | Overall |
|--|---------|
| ESG – Environmental, Sustainability and Governance impacts | 32% |
| Security – Increased cyber security and digital risks | 29% |
| CX – Improving customer experience | 26% |
| Data – Exploiting the value of data across the business | 24% |
| Strategy – Articulating a clear digital strategy | 20% |

Note: n=170

©2023 Omdia

The fundamental challenge is determining the materiality of technology investments to enable ESG outcomes for a broad range of stakeholders, aside from more simple cost out and efficiency improvements.

These constraints become more evident when we assess the degree of plans in motion around major digital projects that address measurable ESG impacts.

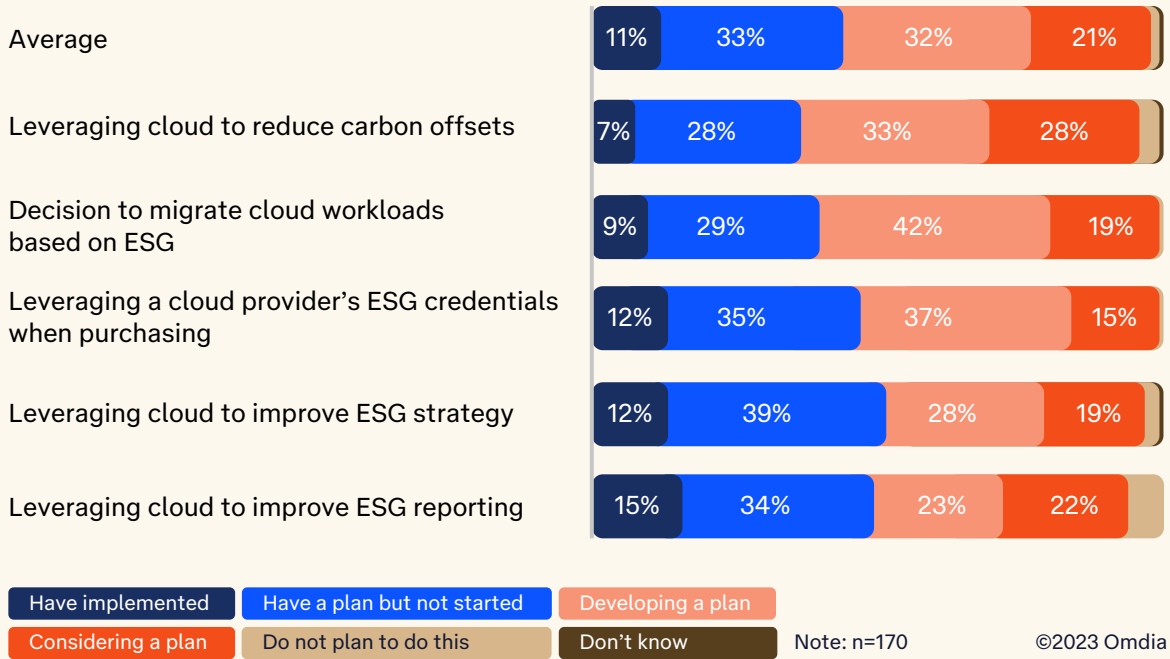
“ Sustainability is paramount for us to reduce our carbon footprint. We are using onsite battery-driven vehicles, biodiesel, and solar. ”

Deputy CISO of a large Australian construction company.

Currently, 97% of firms have or are considering leveraging cloud to positively impact ESG results. However, on average, only 11% of firms have implemented programs that leverage technology-led transformation to support ESG goals. (Figure 7)

In pursuit of sustainability goals, firms are anticipated to prioritise technology investments aligned with their industry goals and broadly, net-zero emission targets.

Figure 7 – How is your organisation considering the role of digital transformation in supporting environmental, social and governance (ESG) goals?



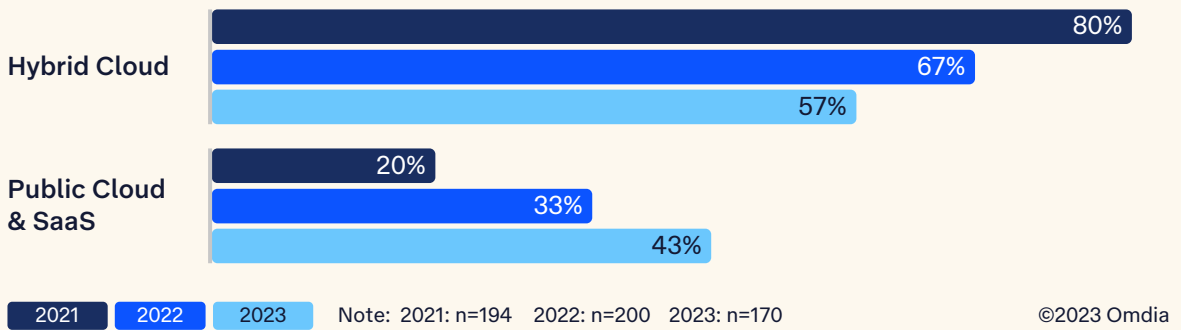
Challenges in preparedness for critical workload migrations to the public cloud

Public cloud adoption continues to grow.

Over the past year, there has been a noteworthy 10% rise in public cloud adoption, which now supports 43% of critical applications in Australia (refer to Figure 8). Despite this growth, the hybrid cloud model (which combines public and private cloud resources) remains the predominant choice for mission-critical workloads. This preference for interconnected clouds, combining on-premises infrastructure with cloud resources, stems primarily from risk and compliance considerations, as well as challenges related to migrating legacy systems, particularly in areas such as storage, business analytics, security services, and industry-specific custom applications.

Australia is fast approaching a turning point in cloud deployment. By 2025, public cloud, including Software as a Service (SaaS), is poised to surpass private and hybrid cloud for essential business applications. This shift will be further accelerated by economic pressures, driving organisations to seek cost efficiencies through consolidation and automation. However, the migration rate is expected to taper as the less complex and lower-risk workloads are addressed first, while more intricate and resource-intensive applications will require a more measured approach.

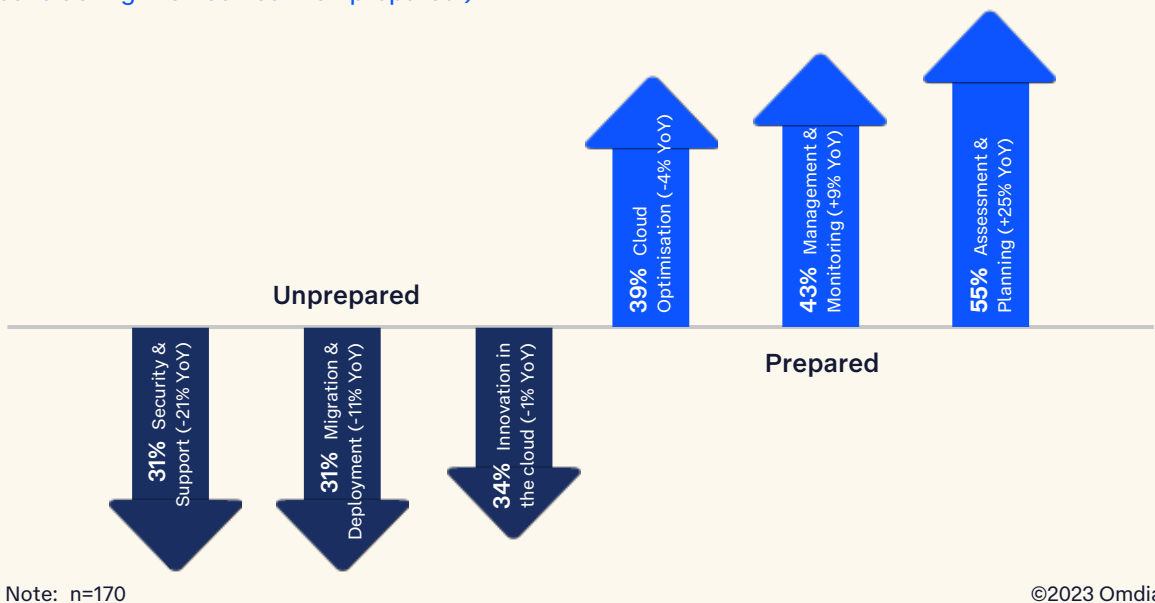
Figure 8 – Current Cloud Usage: What percentage of current business-critical applications are in each type of cloud environment? (Percentage of response across 2021 to 2023)



Continuing cloud migration preparedness falters.

The readiness for continued cloud migration stalls. According to this year's research, 40% of Australian organisations are currently deemed 'well prepared' for the challenges associated with mission-critical cloud migration. This is a slight dip from the 41% reported in 2022. Notably, security concerns, skills gaps, deficiencies in hybrid cloud strategy, and migration risks emerge as the most prominent challenges that organisations are least equipped to handle when migrating critical workloads (see Figure 9).

Figure 9 – How well prepared is your organisation to accelerate the move of critical business applications to the cloud in the following areas? (Percentage of respondents considering themselves 'well prepared')



Faced with more stringent IT budgets, many organisations are increasingly turning to external consulting expertise for design and assessment services to optimise deployment success. The level of preparation at the 'assessment and planning' stage has seen a noteworthy 25% year-over-year increase.

As the adoption of Software as a Service (SaaS) continues to rise, leaders are swiftly embracing cloud management and monitoring solutions to effectively navigate cloud sprawl. However, leveraging the cloud for innovative solutions and ensuring security remains an area where organisations are most notably unprepared. Further insights into this aspect will be explored later in this paper. (Refer to Figure 9 for visual representation)

Skills shortages in the cloud have rapidly escalated as major cloud migration setbacks.

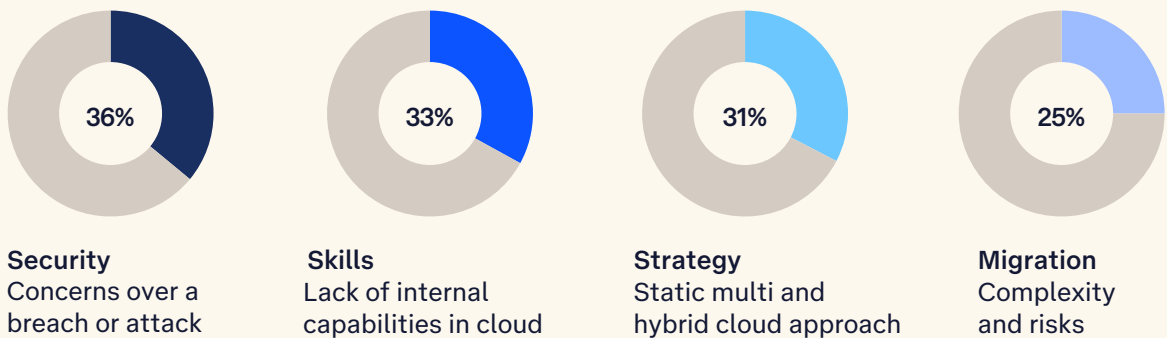
Cyber security remains the most significant concern among Australian executives this year, unchanged from the 2022 research. (Figure 10)

The threat of an attack with material consequences is increasingly likely, elevating security to a standing boardroom agenda item alongside or combined with enterprise risk discussion.

“Lift and shift looks easy but in reality, is hard to implement with legacy systems.”
CTO of a major insurer

In contrast to last year's survey, lack of skills has shot up from ninth rank in 2022, driven by a lack of internal capabilities to modernise remaining, often complex, legacy, and large-scale applications.

Figure 10 – For critical applications/workloads, what are your top three concerns when modernising in the cloud? (Percentage of respondents)



Note: n=170

©2023 Omdia

An adaptive network is crucial for hybrid cloud success.

As organisations navigate the complexities of modern digital ecosystems, they are increasingly recognising the significance of having a network infrastructure that can seamlessly adapt to evolving requirements.

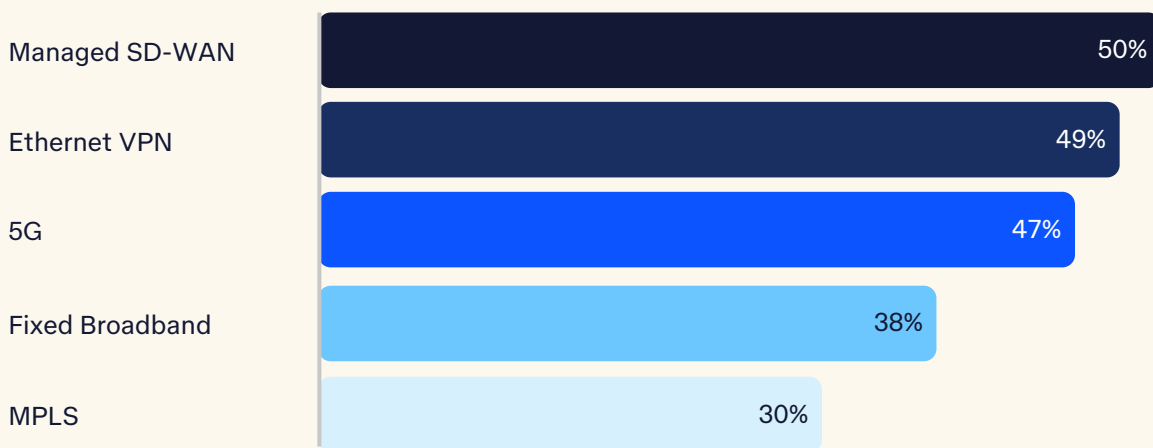
In the pursuit of hybrid cloud success, leading organisations have identified the need for a blend of both virtual and fixed networks to establish robust backhaul connectivity. This strategic combination ensures that data and applications flow efficiently between on-premises infrastructure and cloud-based resources, creating a cohesive and resilient digital environment.

The surge in remote working practices has further underscored the criticality of a well-functioning network. With a distributed workforce relying on cloud-based applications and resources, a reliable network becomes the backbone of seamless operations. Additionally, the heightened interest in edge computing – where data processing occurs closer to the source of data generation – necessitates a network that can facilitate low latency connections to edge devices.

Furthermore, redundancy considerations have become paramount in network design. Organisations recognise the importance of having failover mechanisms in place to guarantee uninterrupted connectivity, even in the event of unexpected network disruptions.

In summary, an adaptive network is the linchpin of success in hybrid cloud environments. By strategically leveraging a combination of virtual and fixed networks, organisations can establish seamless connectivity between on-premises infrastructure and cloud resources. The integration of 5G technology further propels the capabilities of modern networks, enabling organisations to embrace the full potential of digital transformation.

Figure 11 – What type of backhaul network connectivity is most important for your hybrid cloud? (Percentage of respondents)



Note: n=170

©2023 Omdia

Network expertise and security also remain paramount in choosing a managed cloud services provider.

Selecting a managed cloud services provider hinges on their proficiency in network management and security. It entails choosing a provider with a strong track record in ensuring the smooth and secure flow of your data.

A majority of Australian leaders (around 69%) emphasise the significance of robust network skills when opting for a managed cloud service provider. In our discussions with executives, many highlighted that an isolated approach to network and hybrid cloud can hinder quick and efficient task execution.

This is why leaders typically seek out cloud providers known for their expertise in maintaining security (approximately 51% deem this highly important), adeptness in network management (about 39% hold this as a strong priority), and a reputation for innovation (roughly 35% consider this a key factor).

To achieve seamless operations across diverse cloud service types like public, private, edge, and SaaS, expertise in areas such as SD-WAN, hybrid network virtualisation, 4G/5G integration, and the management of IoT and enterprise Wi-Fi is crucial. However, locating professionals proficient in these domains can be challenging and may come at a premium.

Furthermore, given the surge in security incidents and the heightened need for data protection, there is an anticipated surge in the adoption of Secure Access Service Edge (SASE). This approach integrates critical security tools like Next Generation Firewall, Cloud Access Security Broker, Secure Web Gateways, and Zero-trust Network Access into a unified system, streamlining cloud security management.

Sovereign cloud is becoming essential.

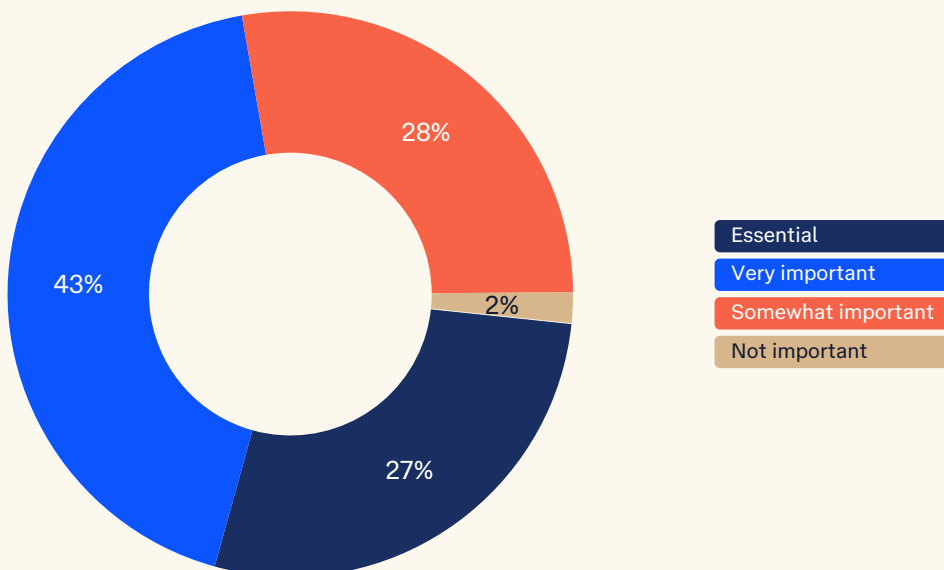
The importance of Sovereign Cloud cannot be overstated. In fact, it has now become a critical factor for the majority of organisations when selecting their hybrid cloud provider in Australia. This is especially true for government agencies and departments, as highlighted in Figure 12.

This surge in significance can be attributed to the paramount concerns surrounding security and privacy. Executives are seeking robust assurances regarding the availability, latency, connectivity, and compliance of their chosen cloud solution. These apprehensions span various critical aspects including localised management, infrastructure, and data residency.

Adhering to recognised standards and frameworks has become instrumental in ensuring compliance with these security and privacy requirements. Notably, the Australian Government Information Security Registered Assessor Program (IRAP), along with frameworks like the Information Security Manual (ISM) and assessments such as ASIO T4, serve as prominent benchmarks in this regard.

In essence, the Sovereign Cloud has evolved from being a preference to an imperative, especially for entities like government agencies. This shift is driven by a collective commitment to safeguarding security, privacy, and compliance in the ever-evolving landscape of cloud computing.

Figure 12 – How vital is sovereign cloud to the choice of your organisation's strategic cloud provider? (Percentage of respondents)



Note: n=170

©2023 Omdia

4.0 On the Edge – Australian firms actively explore the possibilities



Edge computing presents new opportunities

Edge deployments and curiosity among Australian executives are rapidly increasing.

Edge computing is emerging as a platform for innovation across distributed sites, use cases, and industries.

In this year's survey, 33% of firms already run edge computing, up from 22% last year. There are many different and novel use cases emerging. The top five edge solutions currently deployed by Australian organisations are IoT, BI, video streaming and analytics, custom apps, and high-performance computing at remote and branch sites. (Figure 13)

Key industry implementations include: visual analytics in manufacturing/mining, e.g., for worker safety and quality control, energy monitoring and management (e.g., oil/gas with IoT), transport and logistics cases for operational efficiency (e.g., major ports often in combination with private 5G), video streaming for media sector, also AR/VR including for training purposes, patient monitoring in healthcare with data processed at the edge both for latency and compliance reasons.

A common theme in Australia is keeping specific workloads at the edge, data centres or branch offices to overcome latency (and network efficiency/cost) issues, security, and privacy concerns, and get better control over data for compliance reasons.

Encouragingly, over a third of Australian enterprises expect to deploy additional edge solutions in the next 18 months. Many executives are currently considering or experimenting with edge POCs ahead of planned deployments at scale.

Omdia anticipates that the Australian edge ICT services market will experience significant growth, potentially doubling by 2027. This surge is propelled by a diverse range of workloads across key industries shifting towards the edge. This transition promises advantages such as reduced latency, enhanced network cost efficiency, and improved compliance and control.

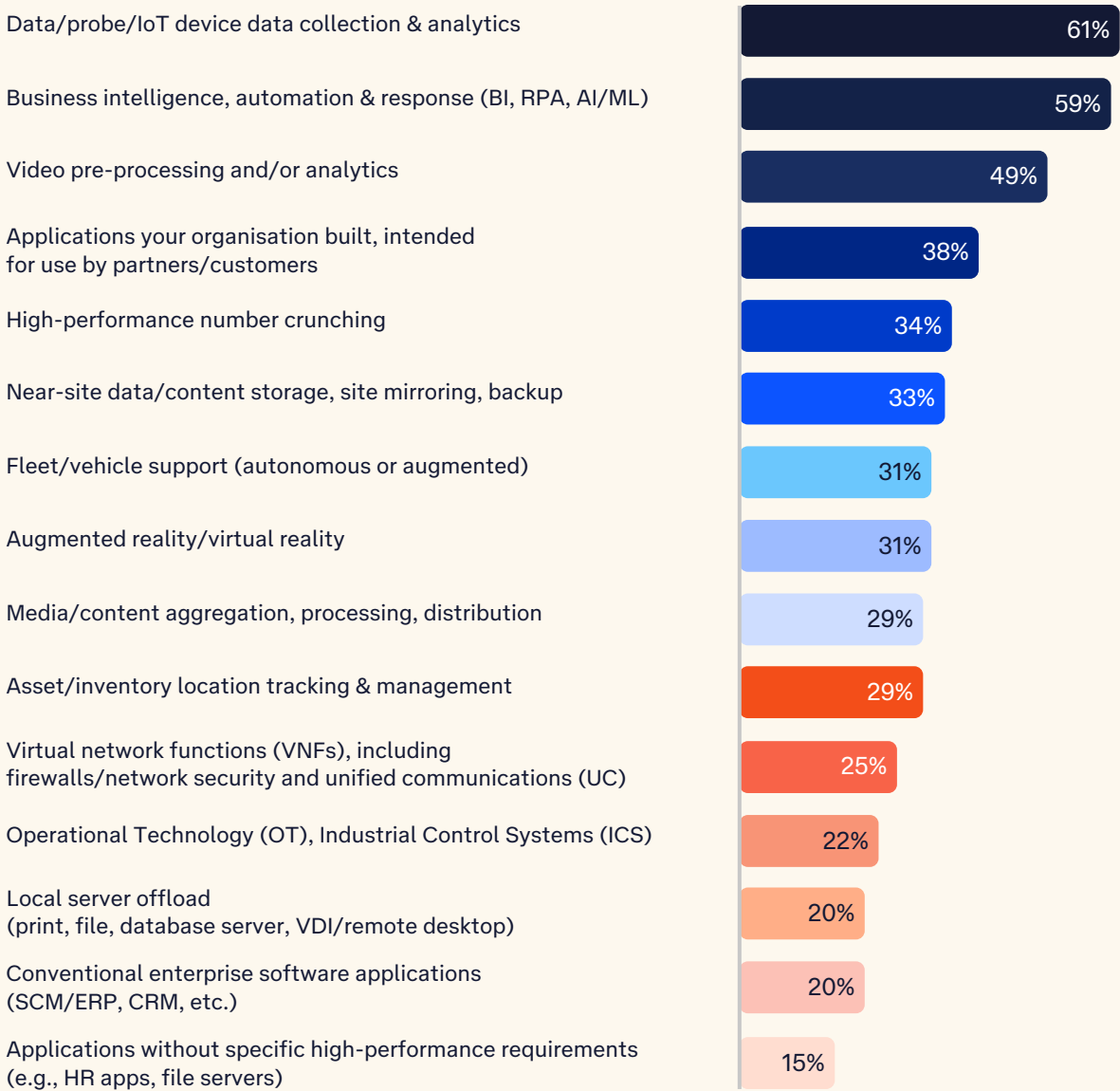
Edge services tend to be integrated with cloud, network and security environments and feature significant portions of consulting, integration, and storage/compute-related third-party services, as well as fully managed edge solutions (e.g., with integrated platforms/applications, analytics, and AI-based workload management tools).

“Right now, edge is very hub and spoke and has been driven by limited bandwidth at remote sites. Our challenge in edge has been firstly our ability to exploit it and secondly the vendors' ability to provide a compelling product.”

“So, for us, edge is a really interesting proposition. I wouldn't say we have exploited its full capability or potential, but very much it's in our mind in an architectural sense and thinking about the future, especially for managing large bandwidth loads.”

CIO at a large Australian utility firm

Figure 13 – What are the top five applications your organisation runs or plans to run at the edge in 12-18 months? (Percentage of respondents)



Note: n=170

©2023 Omdia

Complexity looms large, but growth continues.

Interviews with local executives revealed that the more complex the solution, the more likely it will currently be at the POC stage, not production, reflecting a gap between early trials and mainstream adoption. Also, nearly all executives are interested in edge, but most don't know where to start.

Cost pressures from macro-market conditions are both a constraint and enabler, driving continued interest in how the edge can improve operational efficiency to reduce cost. Still, execs are unclear or stymied by complexity when evaluating the TCO for new use cases.

Most Australian organisations view edge as an operational enabler, not an innovation driver.

An interesting finding from this year's research is that edge adoption rates and expectations are divided between innovation and cost (efficiency).

Statistically, most firms presently leverage edge for operational goals (33%) compared to only 12% for innovation. (Figure 14)

However, in nearly every interview, innovation stood out as the kernel of most new deployments. Australian executives are actively considering, experimenting, and eventually rolling into production novel uses of edge computing, usually combined with hybrid cloud, 4G/5G and now, AI.

Figure 14 – What are the top three business needs in your organisation that are driving, or you expect will drive, the adoption of edge computing? (Most essential, percentage of respondents ranking as first priority)



Note: n=170

©2023 Omdia

The flexibility of the edge cuts both ways.

In this year's research, 39% of organisations cite 'complexity' as the biggest edge adoption constraint, followed by 'security' at 36% and 'cost' at 34%. (Figure 15)

Many edge projects are progressing slowly from trial to production. While trials and POCs are relatively quick to stand up, moving into production introduces possible risks following operational migration.

The flexibility of edge compute capabilities with other emerging tech introduces complexity as edge innovative and successful solutions tend to integrate with other enabling and emerging technologies, including 4G/5G, FWA, IoT, and artificial intelligence (AI).

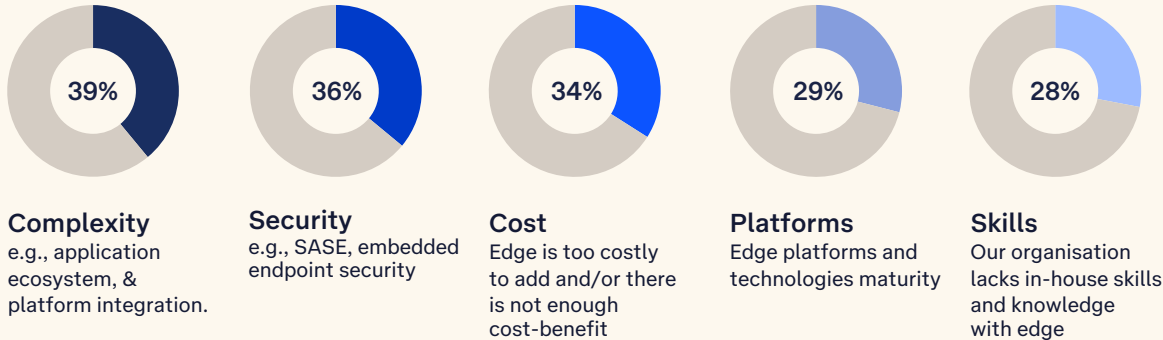
A challenge emerging is that most firms lack the skills in hybrid (fixed/wireless) networking, data and platform integration, and hybrid cloud to make it cost-effectively work at scale, relying on third parties to help design, deploy, and manage aspects of the solution.

“ We would love to be doing edge networking, that's something that is completely in our strategy at the moment...and it's mostly (going to be) followed by a zero trust or SASE framework that we want to implement across our region. ”

Head of IT at a large Australian manufacturer

Our research underscores the pressing need for industry leadership in the field of edge computing, which involves navigating a sophisticated technological landscape. We've identified that concealed complexities, along with their implications for security, can frequently tip the cost-benefit scale unfavourably. This, in turn, obstructs innovation centred around customer experience and hinders the exploration of captivating industry applications.

Figure 15 – What keeps your organisation from embedding edge computing in your digital roadmap sooner?



Note: n=170

©2023 Omdia



5.0 Securing Australia – Cyber Security Challenges and Opportunities



Escalating threat landscape

Surge in high-severity security incidents targeting endpoints, public cloud, IoT and networks.

Concerningly, 61% of Australian organisations have experienced a significant increase in overall security incidents in the last 12 months, up from 57% last year.

Even more concerning is that 23% have witnessed a noteworthy rise in critical security issues within the same timeframe. Notable spikes have been observed in various critical areas, including endpoints, IoT devices, public cloud platforms, hybrid cloud environments, and third-party collaborations (as depicted in Figure 16).

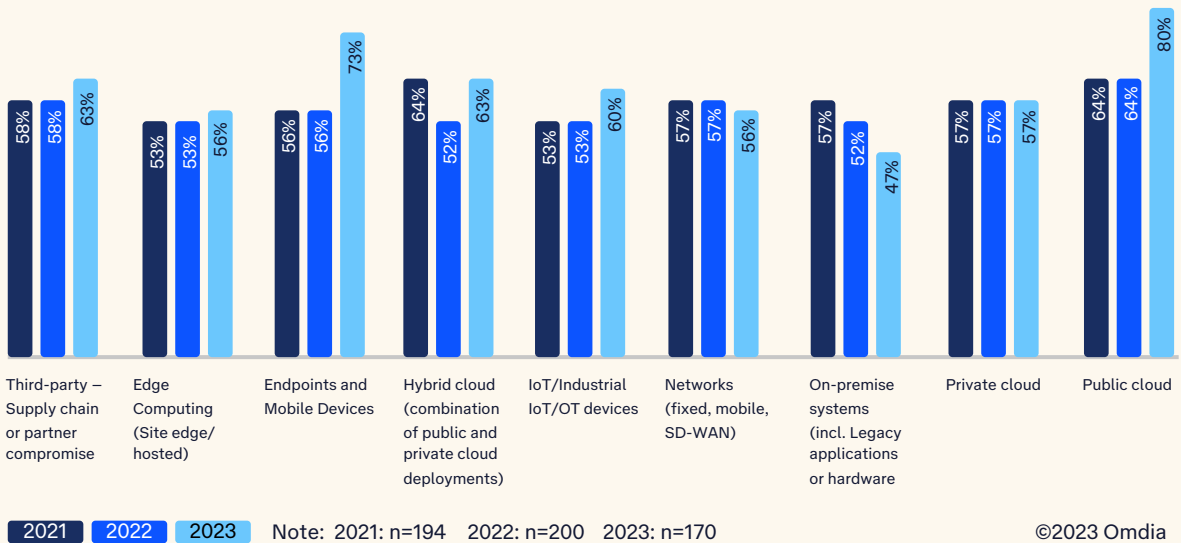
The rapid transition to remote work has introduced a new dimension of vulnerability, resulting in a surge of incidents triggered by endpoints. Simultaneously, the gradual but steady shift towards public cloud adoption has brought about downstream security ramifications.

Notably, the convergence of IT and OT (Operational Technology) is rapidly advancing within industrialised environments. While this integration promises operational efficiencies, it also introduces a new set of security threats that demand our attention both now and in the near future. These trends collectively underscore the urgency of bolstering security measures to safeguard critical assets and sensitive information in today's evolving digital landscape.

“As a financial services company, regulatory compliance such as CPS234 and ASIC banking license requirements mean it's a massive challenge. To be honest it's very extensive and I'm not sure how smaller mutuals deal with it... Regulation results in us needing playbooks and scenarios to be ready, almost accepting there will be a security event.”

CIO at a large Australian financial services company

Figure 16 – Has your organisation experienced a significant increase in security breaches in any of the following areas in the last 12 months? (Comparing 2023 with 2022 and 2021 data)



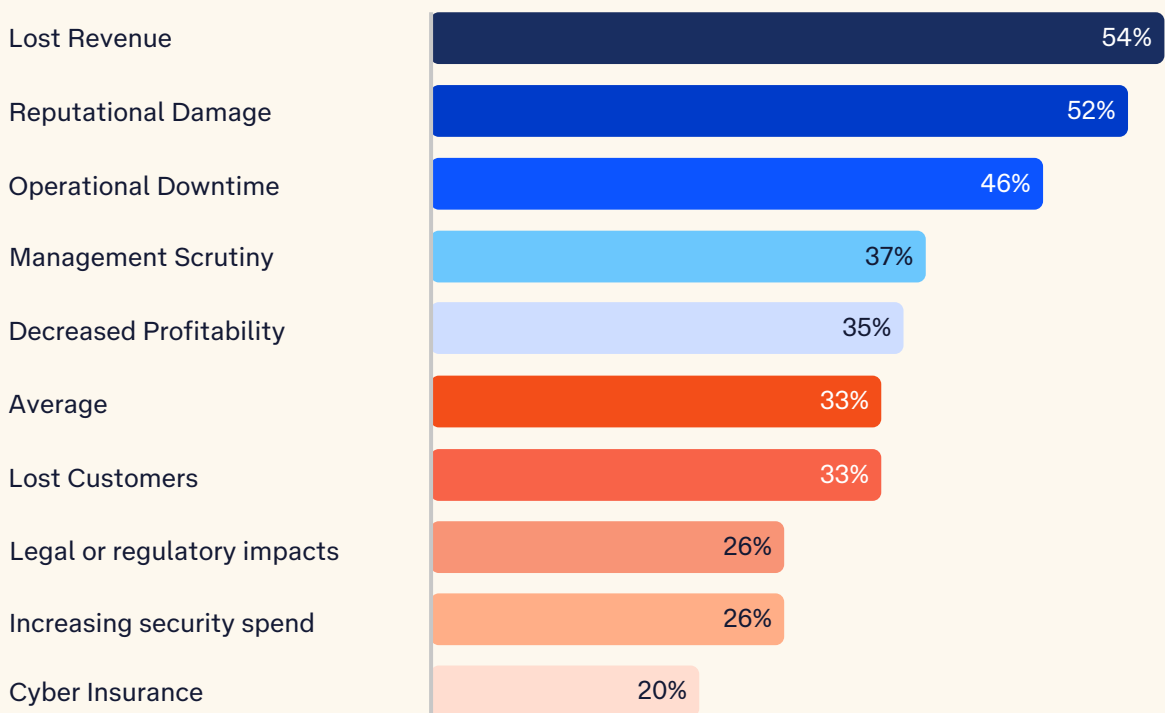
Local leaders indicate material losses from cyber breaches.

A significant number of Australian organisations have experienced substantial losses due to recent cyber incidents. Shockingly, more than a third of these organisations have faced detrimental consequences affecting various aspects of their operations.

Specifically, 54% of Australian firms have reported a decline in revenue, 52% have suffered damage to their reputation, and 46% have experienced operational downtime. Additionally, these incidents have led to increased scrutiny from management, loss of customers, legal consequences, and escalated expenses on security and cyber insurance (as shown in Figure 17).

These negative impacts often occur in tandem. Recent instances of cyber-attacks on IT or OT environments, including ransomware attacks, triggered a series of events such as activating emergency response plans, leading to operational downtime and subsequent revenue reduction. The process of containment and remediation is also costly. Moreover, the damage to reputation has a long-lasting effect, and in some cases, has resulted in the complete shutdown of affected firms.

Figure 17 – What was the impact of the most significant recent cyber security incident or breach on your organisation?



Note: n=170

©2023 Omdia

Quantifying the impacts of a breach.

To provide a more precise assessment of the impacts, we requested organisations to estimate the financial repercussions of significant security breaches related to cloud services that occurred this year.

The research indicates that Australian firms lost, on average, over 10% of revenue from the most recent cyber breach. The impact was also a 19% rise in price pressure passed onto customers or deteriorating margins. (Figures 18-19) Consequently, firms will continue to allocate a greater proportion of funding to cyber security, including network and cloud such as SASE.

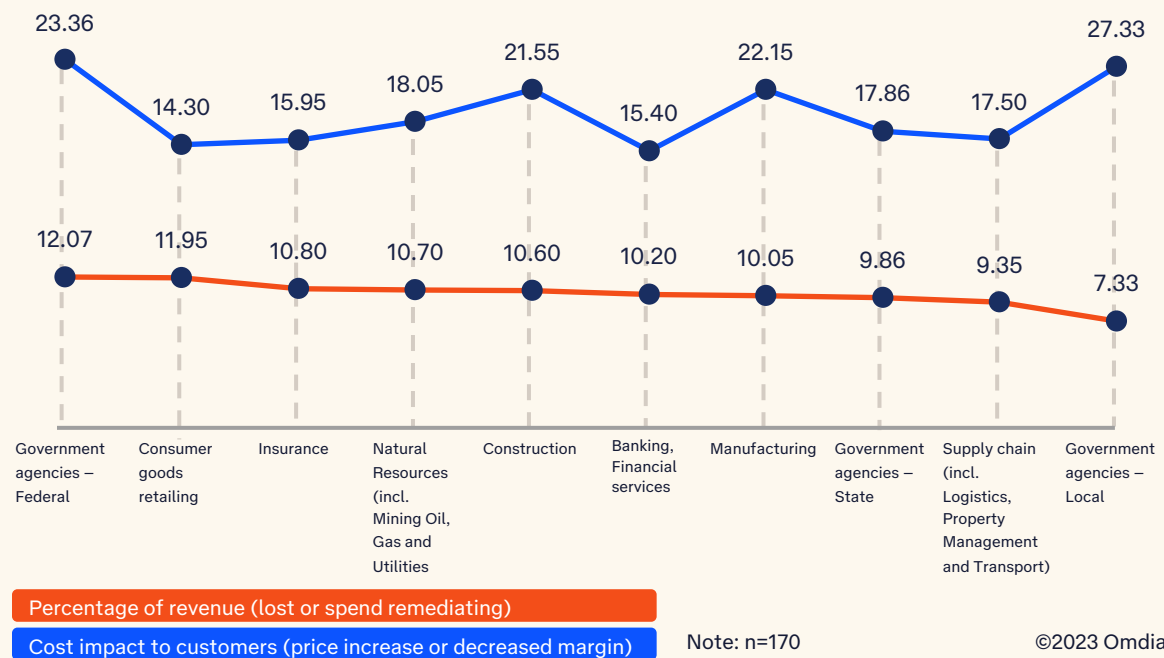
Government agencies were worst hit in absolute revenue terms (notably Federal) and overall cost impacts to customers, i.e., citizens. Arguably, some of every dollar spent remediating emergency security incidents erodes Australia's economic productivity growth. As noted in the ACSC Annual threat cyber report, local and state government agencies had some of the higher number of C3 to C5 level incidents in the 2021-22 financial year.³

Cost-sensitive industries, including construction and manufacturing, also estimate significant cost impacts from recent attacks, mediating operational downtime impacts. Further, heightened risks from connecting IoT/OT with IT environments will push many critical infrastructure sectors to explore integrated SIEM and threat detection across connected environments.

Figure 18 – What was the estimated financial impact of recent major cloud-related security breaches? (Percentage of revenue or margin, all sector average)

| | Overall | Midmarket | Enterprise |
|---|---------|-----------|------------|
| Percentage of revenue (lost or spent remediating) | 10.45 | 9.80 | 11.11 |
| Cost impact on customers (price increase or decreased margin) | 18.80 | 17.87 | 19.73 |

Figure 19 – What was the estimated financial impact of recent major cloud-related security breaches? (Percentage of revenue or margin, sector results)



³ ACSC Annual Cyber Threat Report, July 2021 to June 2022 accessible at <https://www.cyber.gov.au/about-us/reports-and-statistics/acsc-annual-cyber-threat-report-july-2021-june-2022>. Note Category 1 (C1) refers to the most severe risk/incident, through to the lowest at Category 6 (C6).

As we look ahead into 2024, the state of cloud security preparedness remains stagnant.

Only 39% of Australian firms can be deemed 'well prepared', which is the same figure as last year's survey. Additionally, the proportion of leaders who are 'somewhat prepared' has dipped to 42%, down from 51% in the previous year.

This lack of readiness primarily stems from challenges in securing mission-critical cloud operations. More than a third of firms confess to being 'not at all prepared' for integrating cloud with their existing security systems (whether in-house, SIEM, SOC). Additionally, 21% express unease in managing change, and 18% feel less adept at utilising advanced technologies and platforms like SASE.

These findings might be somewhat surprising, considering the substantial investments and emphasis on AI-driven security platforms in the market. It's important to remember that many security platforms charge based on data consumption. As organisations expand their tech infrastructure, the amount of threat data increases, leading to a surge in alerts that require assessment, triage, and action. This dynamic adds an additional layer of complexity to cloud security preparedness.

Outsourced Security Services are on the rise.

As the threat of breaches continues to have significant consequences, the importance of cyber security is on the ascent. Addressing this challenge encompasses all five stages of the NIST framework: identification, protection, detection, response, and recovery.

In response, many executives interviewed are reconsidering or have recently migrated security operations activities to third parties under annuity outsourcing agreements.

With growing threats, and skills shortages in threat detection, response, and recovery across complex IT hampered by slowly growing budgets, security leaders intend to focus on refining their security strategy. Outsourcing and engaging consultants to bolster proactive security posture assessments are gaining interest.

Interviews with security leaders revealed they favour providers that can demonstrate local deep support and capability breadth (consulting and managed services, with subject matter expertise) across the hybrid cloud, edge, and increasingly AI-enabled security platforms.

Key examples include Microsoft Sentinel and Defender, Carbon Black, and Amazon Guard Duty & Shield. Interest in enterprise application security, e.g., for SAP and Oracle, is proliferating as these applications move to the public cloud.

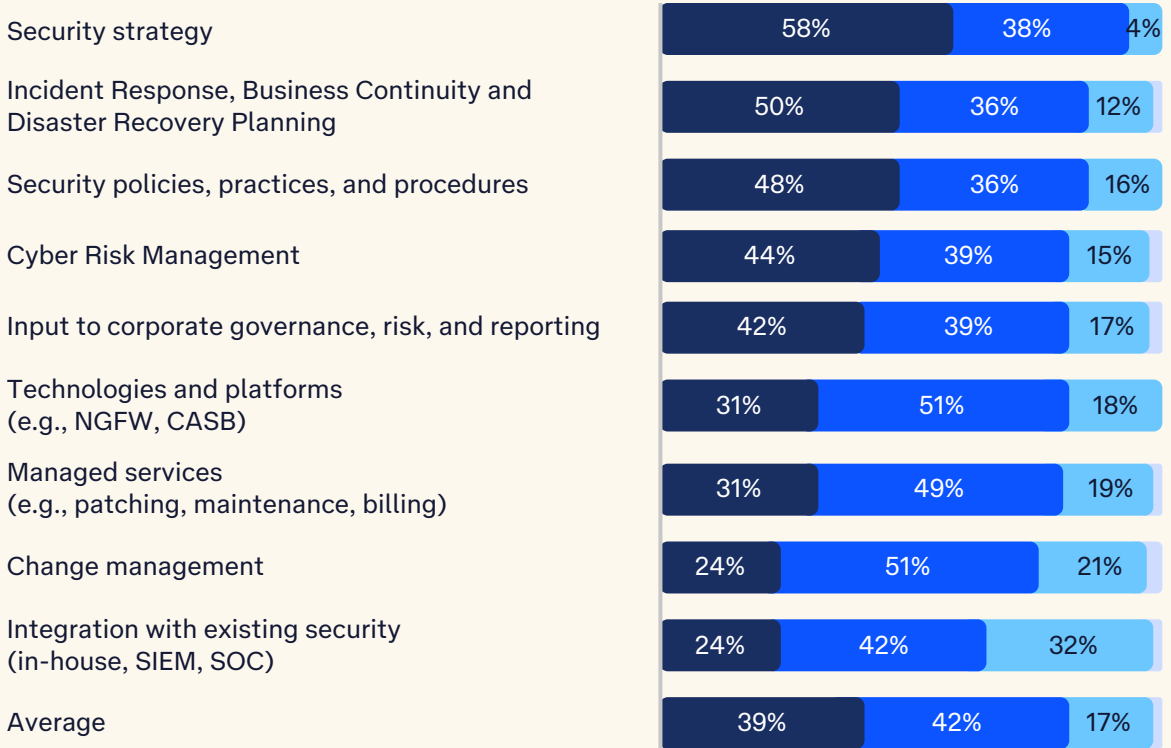
The stakes are rising as more firms move critical workloads to the cloud. Now is the time to act.

“ We won't use a specialised security services vendor. So, I like to keep things simple rather than having multiple vendors because I don't want a position where you know, people are pointing at each other.

On top of that, our industry is complicated. I need someone that's cognisant of all those moving parts and is aware of this industry and has the relationships with some of those other providers to offer end-to-end solutions. ”

CIO at a large Australian financial services company

Figure 20 – How prepared are you, or how effective is your organisation in the following cloud security areas? (Percentage of respondents)



Very Somewhat Not at all Not sure / don't know

Note: n=170

©2023 Omdia

6.0 A Path Forward – Recommendations



Navigating the Way Forward – Insights from Australian decision-makers

In light of insights gathered from Australian decision-makers, it is clear that a strategic path forward is crucial. Executives must remain cognisant and vigilant of challenges, constraints, and varying degrees of preparedness within and across hybrid cloud, edge computing, and security.

Local leaders are tasked with the delicate balance of overseeing IT expenses while aligning with corporate aspirations to foster innovation driven by enhanced customer experiences.

Yet, it's important to acknowledge that this journey is no easy feat. With this in mind, this report aims to shed light on three key focal points that Australian organisations can emphasise to instigate substantial business transformation through technology.



1

Redefine the business case as market pressures mount.

Several leading executives Omdia spoke with were able to clearly articulate and measure the impact cloud plays in enabling a company's broader digital transformation program, not just realising cost savings. This year's research highlights the expectation gap between cost savings and desired innovation outcomes. The most notable achievers have seamlessly integrated cloud into the very fabric of all lines of business-driven enterprise change programs and digital transformation endeavours. They have succeeded in establishing tangible and quantifiable benefits that resonate with the entire organisation, transcending the realms of IT and expenditure. These accomplishments encompass notable enhancements in customer and partner experiences, accelerated time-to-market, enhanced compliance with regulatory frameworks, fortified security measures, and improved site and critical application dependability. All these advancements are achieved while maintaining a vigilant eye on cost management and reduction.

2

Get more proactive with cyber security and network resiliency.

As the rate and impact of security incidents continue to surge, executives responsible for security must prepare for the worst. Scenario planning, response playbooks, proactive security posture assessments, leveraging advanced security tools and ensuring 24X7 SOC coverage are essential.

As Information Technology (IT) and Operational Technology (OT) converge, edge adoption grows, and public cloud adoption races forward, network performance and increasingly cloud sovereignty are paramount decision factors for the choice of cloud providers. Leaders increasingly recognise that a well-designed and tightly managed network is essential to the scalability, resiliency, security, and application performance of any cloud deployment for critical applications.

3

Leverage the right partners to overcome complexity.

While Australian organisations have made significant strides in their digital transformation endeavours, they have yet to fully realise the anticipated advantages. Often, the challenges arise from intricate factors such as covert complexities in application migration, cyber security apprehensions, a lack of transparency, and intricate networking dependencies. Consequently, many leaders are now re-evaluating their approach to partner engagement. Some are in the process of reworking existing agreements, while others are actively planning to enlist external service providers renowned for their proficiency in consulting and managed services. These experts will play a pivotal role in streamlining, automating, and optimising both established and burgeoning deployments.

Engaging partners with robust consulting capabilities can substantially accelerate the journey to value for enterprises. They possess the expertise to cater to industry-specific requirements, navigate around common stumbling blocks, and deliver tangible benefits in a more expeditious manner.

7.0 Appendix



Appendix

Telstra partnered with a leading research firm to conduct this study, offering valuable insights into the experiences of Australian enterprises and government agencies in 2023. This paper aims to provide guidance for technology and business leaders seeking to leverage cloud, security, and edge technologies for sustainable competitive advantage.

Methodology

To better understand the reality of cloud computing, edge, and security among leading Australian organisations, Telstra commissioned Omdia to conduct an independent, comprehensive, local market study on the state of cloud computing adoption in Australia. Telstra's commitment to this research for two years has revealed clear trends and how leading Australian organisations leverage these game-changing technologies for business outcomes.

From March through to June 2023, Omdia conducted a direct primary research survey of 170 executive decision-makers at mid and large-sized Australian companies and government agencies. Small to medium enterprises, 'Midmarket' (>100 to 1000 employees) comprised 50% of respondents, and 50% were large (>1000 employees) organisations. Forty-five percent of respondents were responsible for technology (including CISO, CIO, IT Manager, and Chief Architect), and 55% were business leaders (including CEO, CFO, and COO).

Omdia also conducted in-depth interviews with ten senior IT and business decision-makers responsible for choosing cloud in their organisations to reveal detailed views of executives' cloud aspirations, challenges, constraints, and service provider partner considerations. These interviews are in addition to the dozen conducted for last year's report.

The study reached across industries including, Banking, Financial Services, Insurance, Construction, Retail, Manufacturing, Resources, Mining, and Government at federal, state, and local agency levels. Global counterpoints in this research draw on Omdia's global expertise in its Digital Enterprise Services, Cloud, Data Centre, and Security intelligence services.

Author

Adam Etherington
Senior Principal Analyst

Omdia Consulting

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

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives. Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalise on evolving business models.

Omdia is part of Informa Tech, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange. We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the "Omdia Materials") are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together "Informa Tech") or its third-party data providers and represent data, research, opinions, or viewpoints published by Informa Tech, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an "as-is" and "as-available" basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees, agents, and third-party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.

Get in touch

www.omdia.com

askananalyst@omdia.com




Telstra
Purple



Discover how Telstra can help you securely leverage Cloud and Edge solutions to optimise your business.

 [Request a callback](#)

 [Cloud and Edge Solutions](#)

 [Contact your Telstra Representative](#)