kyndryl

ADAPT

Security and Resilience for a Modern IT Organisation

Why security should never be an afterthought

Author:

Shane Hill, Principal Research Analyst at ADAPT

Introduction

Cloud advancements, an uncertain external operating environment and the realities of distributed workforces have proven the importance of a scalable and agile IT infrastructure.
Chief Information Security Officers (CISOs), Chief Information Officers (CIOs), Chief Technology Officers (CTOs) and Infrastructure Leaders are being forced to rethink business continuity practices and shift to business resilience. This will require business models and operations to change due to the risks that are crystalising with distributed workforces and workplaces. The need for scalable, agile IT infrastructure to support these trends cannot be overstated.

Market Trend

ADAPT's ongoing Cloud Migration study and regular surveys with CISOs, CIOs, CTOs and Infrastructure Leaders illustrates that there is sufficient focus on modernising infrastructure and applications, including migrating mission-critical workloads to the cloud. But security is often an afterthought.
Security remains critical in this complex environment of distributed IT architecture and infrastructure. Modernisation of IT, particularly migration to the cloud, cannot be contemplated in isolation from security. When secure design practices are not applied, increased costs, security vulnerabilities and scope creep may follow.

Market Opportunity

The relative lack of focus on security in cloud migration initiatives presents an opportunity for Australian organisations. Executives must focus on three areas: integrating security into policy and strategy, cloud migration and operations, and skills and deployment. Addressing these opportunities will secure data and workloads and ensure compliance and governance.

Best Practices and Key Outcomes

This report will provide guidance on infrastructure modernisation from a security perspective by examining:

- Best practices for adopting a resilient, secure approach in a modern large organisation.
- The five actions to ensure cyber security and resilience.
- The key outcomes of implementing these actions before, during and after cloud modernisation.

These practices will enable business and technology executives to assess the value of compliant cloud migration to support legacy modernisation and strengthen enterprise resilience.

Market Trend: Modernisation accelerating; security an afterthought

Infrastructure modernisation is a priority for Australian executives

Infrastructure modernisation is a broad concept that means different things to different organisations and the processes of modernising infrastructure will differ depending on the nature of an organisation's business and its starting point—how it currently meets its IT requirements.

The imperatives of IT modernisation are similar across most organisations. Organisations need IT to be more responsive to compete with nimble new competitors not hampered by legacy IT. IT services need to be delivered at a lower cost of ownership and with a higher return on investment. In the face of increasing threats, organisations need to make IT more secure and more resilient—the two are not the same.

The following table describes the top infrastructure modernisation priorities for CIOs and CTOs in 2022.

IT Initiative	CTOs	CIOs
Infrastructure modernisation (compute, storage, network)	Higher Focus: 76% Higher Funding: 37%	Higher Focus: 49% Higher Funding: 19%
Modernise Legacy Applications	Higher Focus: 72% Higher Funding: 34%	Higher Focus: 70% Higher Funding: 28%
Migrate mission critical workloads to PaaS or IaaS	Higher Focus: 65% Higher Funding: 27%	Higher Focus: 40% Higher Funding: 18%
Adopt Software-as-a-Service (SaaS) applications	Higher Focus: 62% Higher Funding: 23%	Higher Focus: 60% Higher Funding: 30%
Move to microservices-based architecture	Higher Focus: 44% Higher Funding: 12%	Higher Focus: 53% Higher Funding: 17%

Source: ADAPT CIO Edge 2022 (133 CIOs) and Connected Cloud and DC Edge 2022 (135 CTOs)

Cloud migration accelerated in the past two years

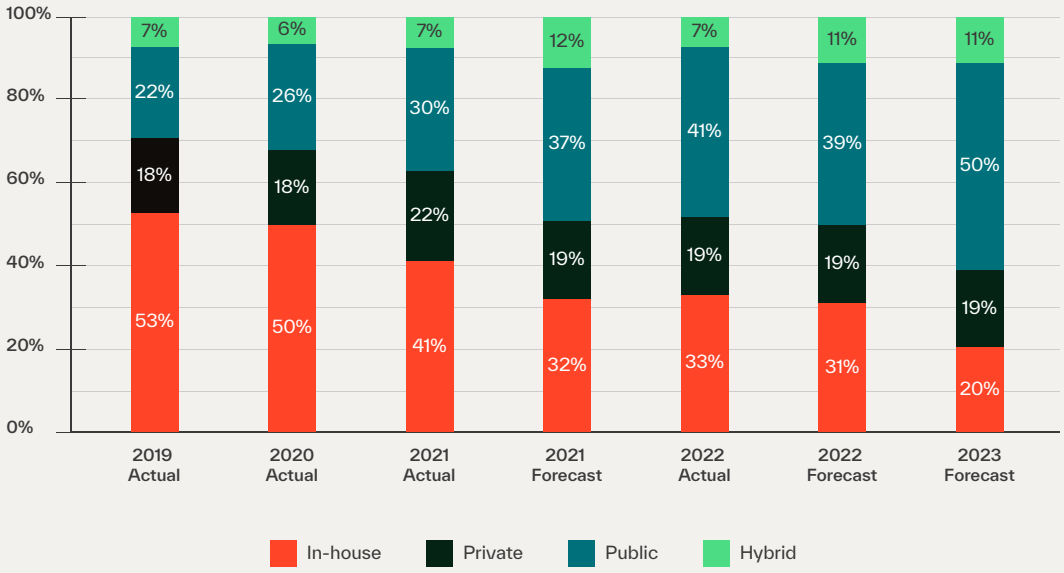
Another aspect of IT modernisation is the move from on-premises to cloud-based applications. The ease with which resources can be brought into service and workloads moved around enables organisations to make their IT much more flexible, secure and resilient.

NAB, CBA, Transurban, Service NSW and many others are already significantly invested in cloud as their core strategy for infrastructure modernisation.

ADAPT has analysed cloud migration trends since 2019, based on the responses of 1,033 Australian technology leaders including CIOs, CTOs and Infrastructure leaders. IT processing capacity steadily moved away from in-house to cloud environments. That shift accelerated in the past two years.

ADAPT

ADAPT Cloud Migration Study



Note: CIOs asked twice a year. Results displayed over an entire year.
Source: ADAPT CIO and CCDC Edge Events 2019 to 2022. Sample Size: 1,033 CIOs and Cloud and DC Leaders

ADAPT finds these specific cloud migration trends arose in the past three years:

1. On-premises workloads were slashed from 53% in 2019 to 33% in 2022, representing a 38% decline in this period.

2. Public cloud workloads almost doubled from 22% in 2019 to 41% in 2022. These actual workloads in 2022 are higher than the 39% forecast for 2022 two years ago.

3. Private cloud adoption remained static, while hybrid cloud workloads sharply increased from 7% in 2019 to 11% in 2022.

4. In 2022, 23% of organisations will have more than five public cloud environments up 4% from 2021. 72% of will have between one and five public cloud environments.

Security is often an afterthought in legacy modernisation

For technology leaders to achieve their key business objectives, they must invest in application modernisation. This will include:

- Migrating mission critical applications to the cloud for complex workloads.
- Increasing the use of SaaS applications for commodity applications.
- Adopting a modular microservices-based architecture for future development.

ADAPT has found that infrastructure modernisation projects often require a move to the cloud in order to replicate the necessary resources—processing power and storage—needed for applications.

Applications should be lifted and shifted or re-architected as appropriate. It is essential in this journey to implement appropriate security controls and ensure IT resiliency in the event of attack. Developing policies and practices, supported with suitable resources can help ensure security and resiliency. Each of these components comes with its own set of security challenges. Security must be maintained when moving and operating applications and workloads into cloud.
The requirement to maintain security during and after cloud migration will include architecting secure data flows. We will detail this requirement in the market opportunity.

ADAPT's ongoing research in these areas indicates that many organisations are not meeting the security requirements of infrastructure modernisation when designing cloud migration programs.

- 56% of CISOs agreed that security features were included at project planning time.
- However, only 45% agreed that security was built into new projects at the outset.

In ADAPT's Security Edge Survey conducted in August 2021, 71% of CISOs identified legacy systems and processes as inhibiting security initiatives. Even though their confidence in the security of the cloud was not high, it did grow. By comparison, ADAPT's Security Edge Survey from April 2022 illustrated that 72% of CISOs thought cloud security would become less of a threat.

Market Opportunity: Address three security priorities

ADAPT finds there are three main areas of security being overlooked, which prevent organisations from embedding security within IT decisions. These opportunities encompass:

- Policy and strategy.
- Cloud migration and operations.
- Skills and deployment.

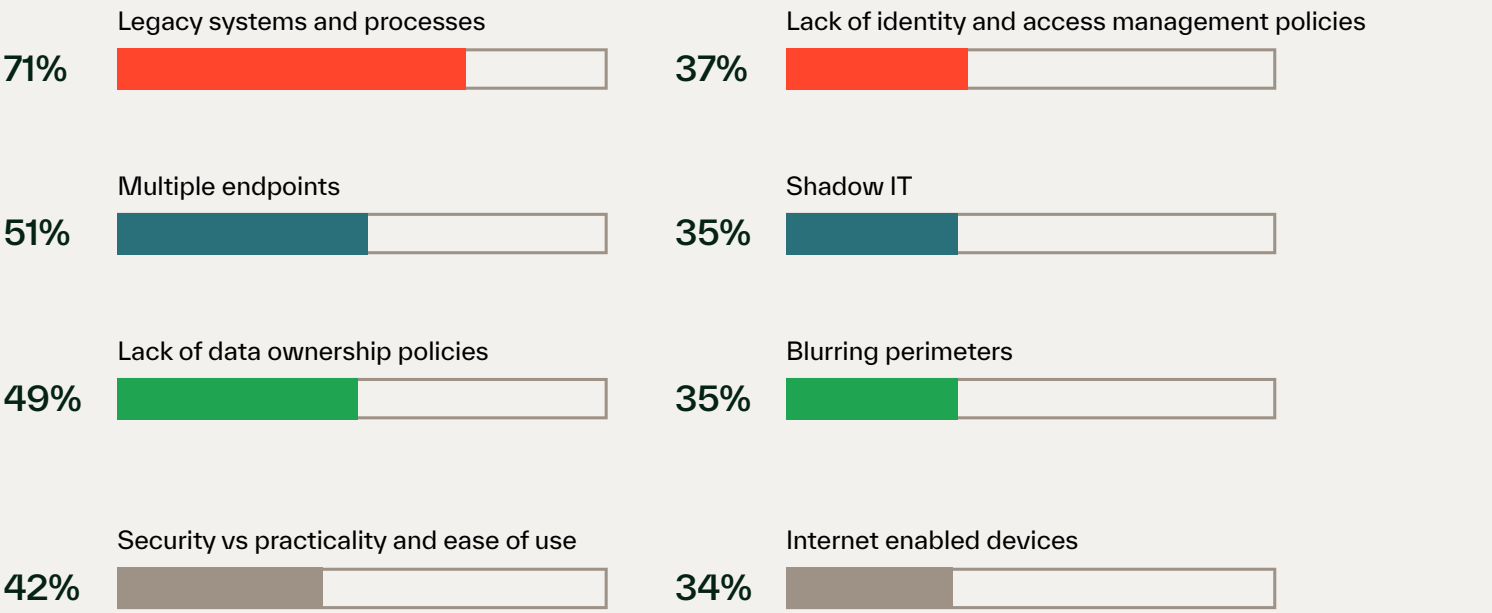
The following passages will describe those opportunities. We will then detail the best practices and key outcomes available to organisations which apply five actions to ensure cyber security and resilience.

One: Policy and strategy

Legacy systems and applications create major technical challenges for Australian CISOs, followed by multiple-end points, complexity of security measures, and data ownership polices. Infrastructure modernisation projects continue to face these challenges, as we depict below.

Technical Inhibitors to Security Initiatives

ADAPT



Source: ADAPT Security Edge April 2022, Sample Size: 97 CISOs and Heads of Security

Most organisations still use localised Security Operations Centre (SOC) policies designed for on-premises systems for cloud migration and operations. Furthermore, there is no clear ownership or governance of data residing in the cloud, back-ups and databases. Especially when workloads are simply lifted-and-shifted to cloud, this poses policy and operational challenges. Auditing and scanning applications before migration and running vulnerability scanners are ways to ensure security policies are embedded into the cloud migration process. These needs can be codified through automation. However, security is brought in much later in the process or there are configuration problems. When a workload is running in the cloud and the User Acceptance Testing (UAT) is underway, no security or resiliency discussion is taking place regarding the backup. It is extremely important for CISOs to elevate these issues much earlier in the migration journey. Questions to ask include:

- When to resume workloads?
- How and when should they be monitored?
- What factors are involved in restoring workloads?

Unfortunately, many organisations only include security conversations as a check in the box during workload discussions. These conversations often occur once migration efforts are well underway.

Collin Penman, Country CISO and Security Practice Leader A/NZ · Kyndryl states:

"Embedding security upfront cuts at least 20% of the time out. If you bring security in post migration, experience shows that could actually double the time needed for the assessment and negatively impact workloads accordingly."

Two: Cloud migration and operations

As a result of moving IT resources from on-premises to the cloud significant security challenges arise, which, unless addressed comprehensively, can leave an organisation vulnerable to a potentially devastating cyber attack.

Kyndryl's Resiliency Practice Leader A/NZ, Sandeep Parande concludes that:
"Disruptions are inevitable. Digital transformation and cloud adoption are leading to an increase in attack surface. Threat actors are becoming stealthier and regulatory compliance requirements are growing more complex."

Due to the sheer volume and variety of their IT resources, many organisations are already burdened with a heavy security workload: multiple applications and management consoles from many vendors create complexities integrating all of this "on-premises spaghetti". Untangling each strand of this spaghetti during cloud migration presents security risks that must be addressed.

Then there are security issues raised using cloud. The organisation no longer has direct control of its IT environment. The tools it was using to secure on-premises resources may no longer be appropriate. While cloud-based collaboration tools like SharePoint and file storage and sharing services like OneDrive have greatly improved the efficiency with which teams can collaborate, they also expose sensitive data to attack by cyber criminals.

Three: Skills and deployment

There is a simplicity in on-premises IT—application and workload deployment—that is often absent in the cloud. On-premises deployment is often centralised; cloud workloads may be distributed across multiple cloud environments. The way an application is supported in the cloud may be completely different from how it was supported on-premises, demanding a different set of skills to secure it.

Before and during the move of an application to the cloud, security needs to be addressed. Before moving an application to the cloud, it must be fully understood how protocols, integration points, business process logic and the application itself work to identify and resolve any security issues.

If the business logic and technical architecture underpinning a piece of software is not fully understood when in its existing, in-house environment, it will not be possible to determine whether any issues that arise when it is migrated to the cloud were pre-existing or created by the migration.

Security integration prior to migration can significantly reduce, by up to 50%, the time taken to migrate the application and ensure it is fully secure and ready for deployment. The more granular the understanding of an application prior to migration the less time it takes to implement the required policies and configure the cloud service.

In Kyndryl's experience, organisations tend to leave important questions about security and resilience to the user acceptance testing stage. Leaving security and resilience until UAT increases the cost to fix any vulnerabilities identified.

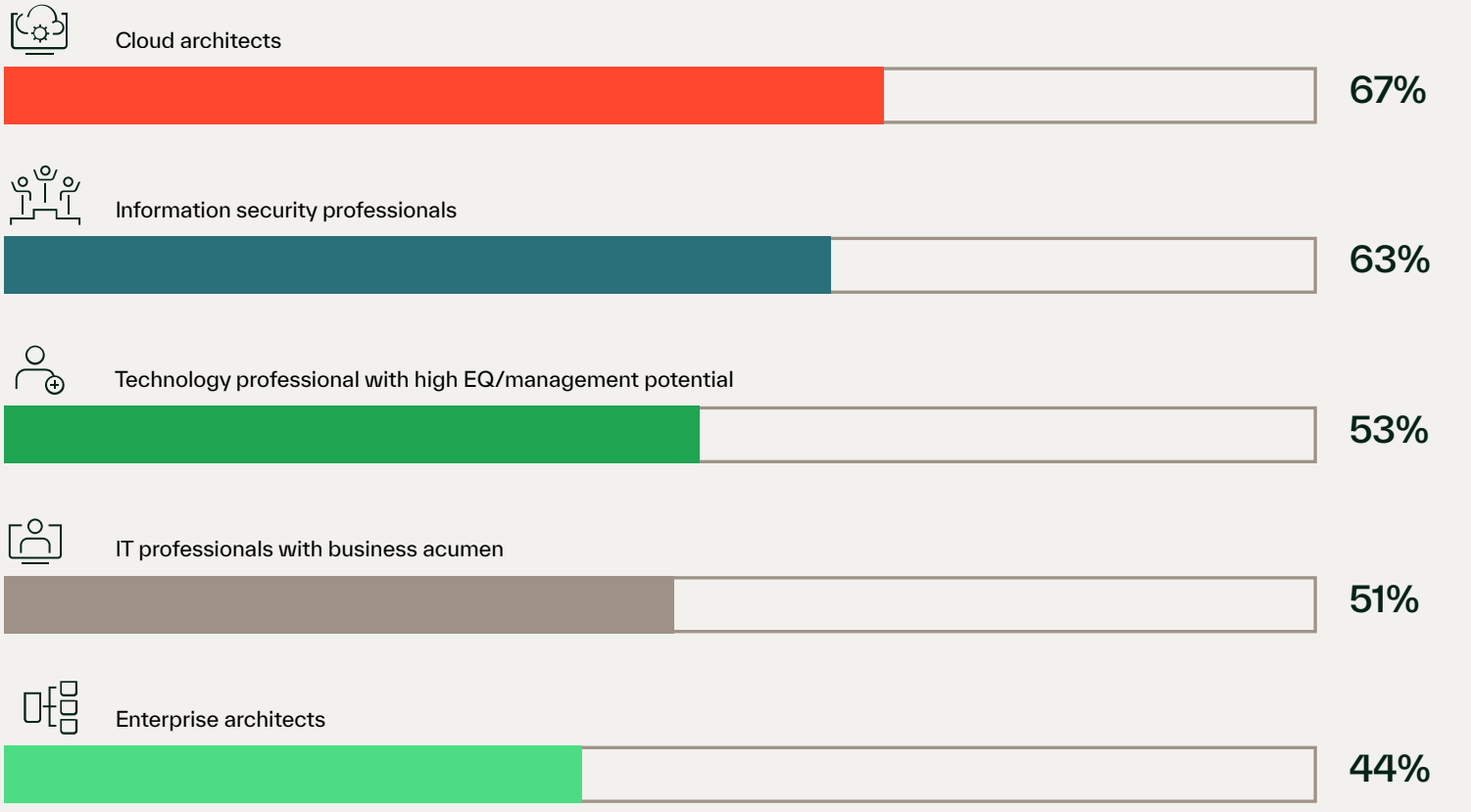
Organisations need to ask questions like:

- How and where is data backed up?
- What procedures should be used for restoring data?
- How is data being monitored?

These challenges are exacerbated by too many manual processes and the existing skills shortage in technology teams. ADAPT finds the two most important skills gaps for Australian organisations are cloud architects and information security professionals, as depicted below.

Most Important Skill Gaps

ADAPT



Source: ADAPT Cloud and DC Edge March 2022, Sample Size: 122 Heads of Cloud, Infrastructure and Technology

Therefore, when thinking about frameworks and best practices around cloud migration, it is essential to consider the resources required to implement best practices. This will enable executives to build a comprehensive automation strategy for Day 2 operations.

Best Practices: How to embed security in cloud migration and operations

In most organisations, the workloads supported by IT are vast, which makes achieving total security virtually impossible. In order to protect the most valuable information, the most critical applications, it is crucial to identify and prioritise the most important assets—the 'crown jewels.'

In the following passages, we will provide five best practices to embed security before, during and after cloud mirgration.

One: Identify the organisation's 'crown jewels'

The failure to identify the 'crown jewels' and prioritise their protection creates two insurmountable problems when a large organisation is involved. The cost of protecting many workloads can be prohibitive and any effective protection strategy would require backups to be maintained. A massive number of backups could take days to restore. Even if an organisation invested heavily in security and resilience, the consequences of a security breach could be dire.

The classic example is a global bank that approached Kyndryl to develop a system to protect and restore workloads in the tens of thousands. During an extensive analysis to identify the bank's crown jewels, the number was reduced to less than 1,000. Those that, if compromised or made inaccessible, would harm the bank's reputation, brand and its business continuity.

Two: Bring Security to the forefront of cloud migration

Embedding security in the migration process is much more efficient and less resource-intensive than addressing security post migration.

Penman states: *"Tackling security upfront will not only accelerate the transformation of the workload, but also leverage the new operating models and advance compliance functionality."*

Activities such as undertaking vulnerability and network assessments during the migration process, examining identity and access management and network protocols, identifying how virtual machines are communicating with each other, determining account ownership and access privileges can save a great deal of time compared to doing all these things post migration.

Gathering more information about a workload, its configuration and applicable policies will simplify migration. This is much easier and more cost-effective than trying to retrofit configurations and policies after migration.

Three: Shift from security to resilience

Australian organisations either do not understand the distinction between cyber security and cyber resilience, or, if they do, do not allocate resources appropriately between the two.

The key differentiators between cyber security and resilience are in an organisation's ability to:

- Respond—undertake appropriate actions to minimise the impact of cyber security events.
- Recover—undertake appropriate actions to restore services affected by cyber security events.

Since 2016, the Australian Securities and Investments Commission (ASIC) has produced several survey-based reports on cyber resilience for firms in Australia's financial markets, the latest in December 2021. Participants were asked to reassess their cyber resilience using the NIST Framework and measure their progress against earlier targets.

The NIST Framework allows a firm to assess its cyber resilience against five functions—identify, protect, detect, respond and recover—using a preparedness

scale that represents where it is now and where it intends to be in 12–18 months' time.

ASIC concluded: "while management of cyber security risk [is] steadily improving overall, there [is] still opportunity for improvement across the entire sector. There is a slight improvement of 1.4% in the overall cyber resilience of firms operating in Australia's financial markets. However, this falls short of the 14.9% improvement targeted by respondents for the period [since 2019]."

Around 15% of respondents to ASIC's survey rated their response planning as only partial or risk-informed, rather than repeatable or adaptive. These maturity levels span four stages, including:

- Partial: policies and procedures are not formalised and responses are reactive.
- Risk-informed: policies and procedures are rarely updated and are not followed consistently.
- Repeatable: policies and procedures are approved, followed and regularly updated.
- Adaptive: policies and procedures evolve in response to changes in cyber security threats.

The percentage of those who have only partial or risk-informed recovery has increased from 2% to 10% since the last survey.

Four: Strengthen disaster and cyber recovery plans

Even a comprehensive and well-tested disaster recovery plan is difficult to implement. One large bank's disaster recovery plan involved 220 steps on a spreadsheet a few years ago. The challenge is executing this correctly under the pressure of a major outage. There is no amount of planning or rehearsal that can fully prepare an organisation for such a possibility. In theory, rehearsals are planned, and all key personnel are available. This is unlikely to happen in reality.

If an organisation cannot recover rapidly and efficiently, the investments in cyber security and resilience will be wasted. Value must be measured in the impact on operations and on customers.

Automation can help. Kyndryl takes these 220-step spreadsheets and converts them into an end-to-end automated recovery engine that will perform the steps needed for a complete recovery, such as shutting down databases, starting workloads, configuring the network and bringing up systems.

Five: Adopt RPO and RTO methods for recovery

Two key measures of cyber resilience are:

- Recovery Point Objective (RPO).
- Recovery Time Objective (RTO).

The RPO is a measure of how old the most recent backup must be in order to enable normal operations to resume in the event of system failure or data loss.
The RTO is determined by the time an application, system and/or process can be down before it causes significant damage to the business, plus the time spent restoring the application and its data.

If the RPO is two hours, snapshots of key data must be taken every hour or 90 minutes, but in today's cyber threat landscape, this does not guarantee that the RPO could be achieved. Today's cyber attackers, once they have penetrated a network, are able to identify the location of backups and encrypt them along with production copies.

In order to guarantee a RPO, it is necessary to use immutable storage: write once, read many (WORM). Once the data is written it cannot be changed until a certain period of time has elapsed.

The integrity of these copies, however, cannot be taken for granted. It is always possible they were created with corrupt data, so periodic scanning is essential to ensure their integrity and restorability. It took a large US credit bureau seven days to work its way through its WORM backups to find the most recent clean version after implementing a WORM system.

Key Outcomes: Five Actions for Secure Cloud Modernisation

The pandemic has taught us the value of becoming more proactive in many areas of our operations. Adopting a more proactive security and resilience posture will recognise the criticality of not just responding to a challenge or threat, but the need to reduce the impact as and when it does happen. A modern organisation will have a proactive cyber strategy that addresses security and resilience together. Failing to address both of these areas will mean that the organisation cannot be truly secure.

Adopt the five actions of cyber security and resilience

Now is the time to recognise and prioritise these five interconnected actions of security and resilience as part of an organisation-wide strategy. These actions will span five areas:

01 **Identifying and agreeing the organisation's 'crown jewels.'**

02 **Using DevSecOps to position security at the forefront of cloud migration.**

03 **Adopting automated compliance to evaluate where the weakest links exist.**

04 **Rethinking how to identify and predict when attacks may happen.**

05 **Implementing and testing cyber recovery site for operational resilience.**

Identify the ‘crown jewels’; prioritise by impact

Organisational security and resilience is a team sport that will require input and buy-in from across the organisation beginning with identifying and agreeing on the key assets, the organisation’s crown jewels. These assets will include infrastructure, information, or a combination of both. Recognise and agree the actions that will have the biggest impact on operations and financial performance, both short- and long-term. By reviewing these impacts, Security and resilence leaders can work with other technology and business unit leaders to determine the crown jewels of the organisation.

Adopt DevSecOps to ensure security is delivered by design

Efficiency and effectiveness are essential when implementing and adapting these security and resilience actions; organisations should implement DevSecOps practices to secure and streamline operations. In DevSecOps, security is viewed as a shared responsibility between developers, operations, and security teams throughout the entire IT lifecycle. As we move more workloads to the cloud to reduce legacy reliance, organisations should leverage DevSecOps to help them implement security by design, in order to secure and streamline operations.

Use automation and cyber recovery sites to predict and mitigate risks

Security leaders need to rethink automated compliance to mitigate future risk, while building the capability to predict when an attack might happen. These leaders must also work collaboratively to identify where the weakest links to the crown jewels exist, and how to quarantine and recover assets before they become unrecoverable. Implementing a cyber recovery site needs to be incorporated into the organisation-wide disaster recovery strategy.

According to Parande:

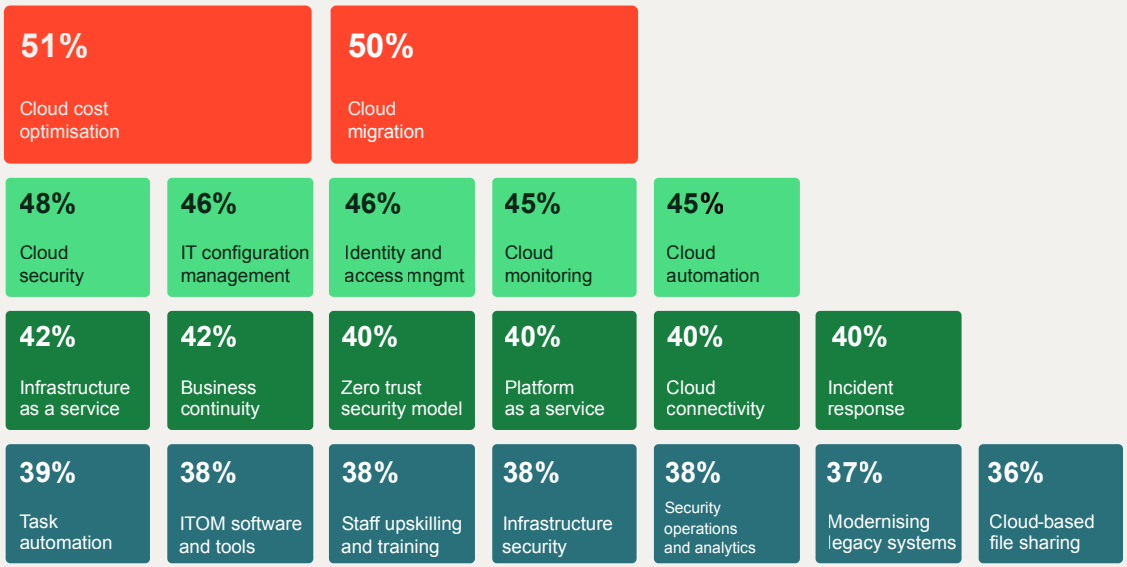
“Organisations need comprehensive resiliency solutions and services to help mitigate business continuity risks across all parts of the hybrid IT environment, enabling them to achieve business outcomes through digital transformation.”

If properly applied, this shared responsibility can ensure security, resiliency and compliance with regulatory requirements are incorporated into application development and application migration processes. This significantly streamlines innovation and operations.

Conclusion

2022 Top Investment Priorities for Cloud and Data Centre Leaders

ADAPT



Source: ADAPT Cloud and DC Edge March 2022, Sample Size: 122 Heads of Cloud, Infrastructure, and Technology

In Australia, CISOs, CIOs, CTOs and Infrastructure leaders place a high priority on security and cloud. Organisations must create a detailed plan to make security a part of cloud and IT infrastructure design.

As Penman states:
"Cloud is the enabling transformation platform for business today and security must become a differentiator in that journey not an after-thought."

The most important drivers for security are data privacy and customer trust. Cloud security and privacy can no longer be an afterthought, these requirements must be built into migration plans from the start.

About Kyndryl

Embrace a 'cyber resilience by design' approach to secure your digital business

Security and Resiliency Services from Kyndryl helps you embed cyber resilience into your broader IT and operational strategy. Enable your organisation to become cyber resilient by leveraging a diverse portfolio of solutions that can help you to:

Anticipate - Achieve and maintain compliance through consistent application of security policies and controls, process testing, audit support, compliance verification, and analytics with Security Assurance Services

Protect – Protect identities, networks, applications, endpoints and data against internal and external threats across your digital initiatives with Zero Trust Services

Withstand - Detect, triage, investigate and respond to advanced threats with Security Operations and Response Services

Recover - Minimise the business impact of unplanned outages with fast, reliable, and scalable recovery across hybrid multi-cloud environments with Incident Recovery Services

ADAPT

About ADAPT

ADAPT's vision is to make Australia & NZ more commercially competitive and productive, for us and for future generations. For over 10 years, we have enabled this by connecting and equipping executives with the knowledge, relationships, inspiration and tools they need to gain advantage. With a deep understanding of modern business challenges, ADAPT deliver unique local research and advisory.

For more information visit adapt.com.au

hello@adapt.com.au
+61 (2) 9435 3535