

A D A P T

Best Practices

Five Actions to Connect, Resource and Secure a Resilient Data Architecture



Written by



Pooja Singh

Senior Research Analyst at ADAPT

Pooja is an expert in technology research and advisory, with a focus on areas such as AI, ML, Cloud, and the business value of Emerging Technologies across different sectors, such as in Healthcare.

In her role Pooja offer insights and helps C-Level end user clients and their strategic partners to meet their mission critical priorities.

Pooja supports these persona in her written research and offering insights on best practices, case studies, market trends, and can advise about strategic sourcing decisions.

Pooja is familiar with technology markets worldwide, with a specific focus on the Australian and South Korean markets.



Aarjun Kumar

Junior Data Analyst at ADAPT

As a junior data analyst, Aarjun is responsible for aiding the analyst team, by gathering and crafting accurate, and relevant insights used at ADAPT's Edge Events and by the Research and Advisory Team.

Having gained a solid academic foundation in data analytics, Aarjun aspires to observe the tips and tricks of data analysis, statistics, and data visualisation to leverage ADAPT's variety of data sources, and inform organisations of the latest challenges, business-oriented pain-points and peer-rated business priorities.

Outside of ADAPT, Aarjun is an active member of Toastmasters International, where he has won speech competitions for his Toastmasters club.

A D A P T

ADAPT is a specialist Research & Advisory firm providing local market insights and benchmarking data to ANZ's senior technology and business community.

Since 2011, we've been empowering the leaders of the region's top enterprise and government organisations to stay at the forefront of modern trends and build for the future.

Our industry leading conferences, private roundtable events and custom research projects equip business leaders with the knowledge, relationships, inspiration and tools they need to make better strategic decisions.

Contact Us

adapt.com.au | hello@adapt.com.au

Table of Contents

- Introduction** 06
- Five Actions to Connect, Resource and Secure a Resilient Data Architecture** 07
 - 1. Engage with stakeholders to demonstrate the value of secure change 07
 - 2. Assess skills and cultural gaps to build the right IT and business competencies 12
 - 3. Build a data-driven organisation through safe and secure behaviours 16
 - 4. Review your specific vulnerability portfolio to create an adaptive defence framework.... 20
 - 5. Ensure the interoperability of people, processes, and technology with security at its core.. 24
- Executive Actions** 28

Build

a data-driven organisation
through safe and secure
behaviours.

Assess

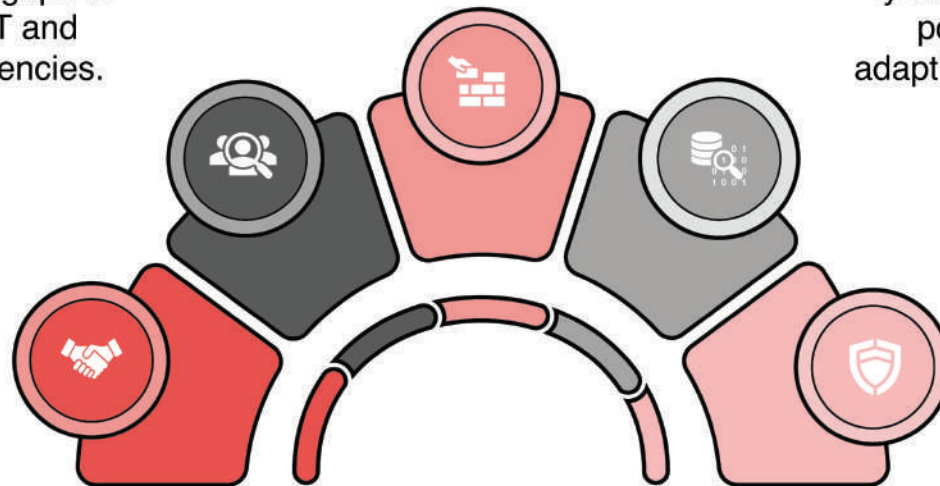
skills and cultural gaps to
build the right IT and
business competencies.

Review

your specific vulnerability
portfolio to create an
adaptive defence framework.

Engage

with stakeholders to
demonstrate the value
of secure change.



Ensure

the interoperability of people,
processes, and technology
with security at its core.

Building a secure and trusted organisation is the number one business priority for Australian Chief Information Security Officers (CISOs) in the next 12 months.



It is also the number two priority for Chief Information Officers (CIOs) and number five for Chief Data Officers (CDOs). To align the activities of security staff with the architecture and resiliency requirements of building a secure and trusted organisation, ADAPT contends that CISOs should adopt these five pillars for success:

- 1**
Best Practice One
Engage with stakeholders to demonstrate the value of secure change
- 2**
Best Practice Two
Assess skills and cultural gaps to build the right IT and business competencies
- 3**
Best Practice Three
Build a data-driven organisation through safe and secure behaviours
- 4**
Best Practice Four
Review your specific vulnerability portfolio to create an adaptive defence framework
- 5**
Best Practice Five
Ensure the interoperability of people, processes, and technology with security at its core

This report describes how these five practices can help enable CISOs to articulate the imperatives for safeguarding, architecting and resourcing a secure and resilient organisation.

1 Best Practice One

Engage with stakeholders to demonstrate the value of secure change

ADAPT surveyed 158 CISOs in April and October 2022, where respondents indicated low engagement at multiple levels of the organisation for cyber security. Less than 50% of CISOs actively communicate security updates to executive leadership and the Board on a quarterly basis.

These low engagement levels are also observed with employees, as only half of CISOs are communicating with employees on a monthly or weekly basis to discuss their role in combatting threats.

1 Best Practice One

The research indicates a need for better frequency and quality of engagement at the upper echelons of the organisation, where CISOs can articulate the state of cyber security and the opportunities to safeguard business value.

These engagements will:

- **Help to gain the buy-in and funding** required from the executive leadership team and Board to show how security can reinforce the organisation's vision and mission.
- **Provide guidance for employees,** both within the security team and across the broader organisation, in a way that enacts these aims in a simple and secure manner.

These challenges aren't new, in fact in an *ADAPT Community Interview* published in September 2019, Digital Champion, Author and Advisor Simon Waller stated:

“

It's important for CISOs to move from their technical language to a common business language.”

Frequency of Meeting About Security Updates

	Never	Once or twice a year	Quarterly	Monthly	Weekly
CEO	19%	28%	28%	22%	3%
Board Members	21%	28%	40%	11%	0%
Executive Leadership	8%	15%	35%	34%	8%
Middle Management	10%	11%	15%	38%	26%
Employees	15%	19%	16%	25%	25%

Source: ADAPT Security Edge 2022: 158 CISOs and Heads of Security

1 Best Practice One

Actions for CISOs to connect and communicate the value of secure change

CISOs who connect the priorities of the executive leadership team with actions for employees will effectively communicate the value of securing the organisation to both of these audiences.

To succeed, ADAPT recommends the following actions with executives and employees:

- **Focus on the business value** (resilience, proactive defence) of security investments. Learn how in the third recommendation of this *ADAPT Market Trends report* published in November 2022.
- **Align and prioritise security initiatives** according to the vision and mission of the organisation to contextualise the costs of these programs related to their positive outcomes.

- **Develop a common language** to relate these investments to the needs of other executives. This language will create a shared understanding of the risks, cost savings, and market advantages.

These imperatives are highlighted in an *ADAPT Case Study* published in January 2022. iNova Pharmaceuticals Director of Technology and Business Transition Michael Smit describes their essence, stating:

Executives do not want change for the sake of change. Making people's lives easier is key to changing perceptions.

1 Best Practice One

Cultivating awareness with employees:

- **Develop security awareness programs** that will fit the needs, experience and interest of employees in IT and, crucially, provide relevance by role for business users.
- **Identify change champions** in the business teams who have the most impact on organisational security. Enlist those who understand the imperative for change and can spearhead communication of the organisation's security agenda within their teams.
- **Highlight**, in clear and relevant terms, how individual behaviors and actions can impact the overall organisation's security posture.

Cultivating this awareness is described in an *ADAPT Case Study* published in October 2022.

That report focuses on how organisations can shift security awareness into a whole-of-organisation effort, in that:

“

**A course that informs mindsets ...
become[s] a beautiful soft diplomacy thing.”**

These actions are the next steps for CISOs to build a secure and resilient organisation.

By improving engagement and demonstrating the value of security, CISOs:

- **Establish a compelling case** for investment in IT skills and technologies. Grow success and engagement in cyber security programs by helping executives lead the shift to a secure culture.
- **Demonstrate value**, influencing behavioural change among the employees to improve their cyber security awareness.

The following practice will explore these actions in more detail.

2 Best Practice Two

Assess skills and cultural gaps to build the right IT and business competencies

Insights from an *ADAPT Market Trends report* published in April 2022 indicate that the workload, and therefore fatigue, of security teams is on the rise. Furthermore, an *ADAPT Persona Mapping report* published in June 2022 reveals how the lack of in-house security skills is the number two barrier to the success of security initiatives.

These barriers experienced by CISOs, and their teams, are shared by Australian CIOs. These common talent challenges are revealed in an *ADAPT Persona Mapping report* published in March 2022, suggesting that Australian organisations are contending with these four talent themes:

1. A need for greater business acumen across technology teams, not just in security.
2. Improved cyber security awareness, competencies and action.
3. The ability to integrate and secure hybrid, multi-cloud systems.
4. Greater aptitudes and abilities in data architecture and science.

Significant IT Skill Gaps in Technology Departments



Source: ADAPT CIO Feb 2022, 128 CIOs and Heads of Technology

2 Best Practice Two

A CIO in the industrials sector described, in an *ADAPT Workshop Recording* published in November 2021, that:

“

We have security functionality, but [because] we don't have a security team, we need to incorporate that into [our] general [technology] team.”

Actions to bridge the cyber security talent and awareness gap

To address ongoing skills shortages, CISOs must upskill existing employees and revisit their talent sourcing strategies.

This will reduce workload and fatigue, improve risk assessment and management, and minimise oversights caused by rushed deployments.

CISOs should:

- **Work with the Chief Human Resources Officer (CHRO)** to embed cyber awareness into organisational learning and development programs. Focus on roles involving analytical, data and behavioural competencies.
- **Partner with tertiary education providers** to offer structured career pipelines and relevant lifelong learning. As described in the *ADAPT Case Study* referenced earlier, focus more on critical thinking and cultural change, and less on complete reliance on technical competency.
- **Develop diversity and inclusion programs and gender outreach programs**, per ADAPT's advice in *Women in Security* published in October 2022. Aim to create a mix of experience and demographics to identify, prepare for and solve problems proactively.

2 Best Practice Two

These actions are foundational. Their foundational nature is described in an *ADAPT Expert Presentation* published in February 2019. In the presentation, Equifax CISO Jamil Farshchi advised:

When you have a talent mix that is 70% administrative skills and 30% [technical], then you have a problem. Your technologists [must] be able to fight [business] breaches.

3 Best Practice Three

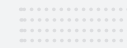
Build a data-driven organisation through safe and secure behaviours

ADAPT research conducted with 638 Australian business executives in 2022 illustrates the shared prioritisation for building the data-driven organisation.


























The research reveals that this is among the top five priorities for CIOs, CDOs, CFOs and, perhaps unsurprisingly, Data Leaders. CISOs, as depicted below, list this as their number five business priority.

Australian organisations generate an enormous amount of data.

CISOs and their executive peers will gain business value from safely and securely securing this data to improve decision making, protect customer trust, and enhance operational effectiveness.



Top Business Priorities for Australian Executives

Persona	1	2	3	4	5
CISO	 <p>Building a secure and trusted organisation</p>	 <p>Improving operational effectiveness</p>	 <p>Attracting and retaining talent</p>	 <p>Ensuring compliance and governance</p>	 <p>Creating a data-driven organisation</p>
Digital Leader	 <p>Attracting and retaining talent</p>	 <p>Digitisation of workflows and process</p>	 <p>Improving operational effectiveness</p>	 <p>Acquiring and retaining customer</p>	 <p>Creating a data-driven organisation</p>
CFO	 <p>Attracting and retaining talent</p>	 <p>Improving operational effectiveness</p>	 <p>Acquiring and retaining customer</p>	 <p>Creating a data-driven organisation</p>	 <p>Digitisation of workflows and process</p>
CIO	 <p>Attracting and retaining talent</p>	 <p>Building a secure and trusted organisation</p>	 <p>Creating a data-driven organisation</p>	 <p>Acquiring and retaining customer</p>	 <p>Improving operational effectiveness</p>
Data Leader	 <p>Creating a data-driven organisation</p>	 <p>Improving operational effectiveness</p>	 <p>Acquiring and retaining customer</p>	 <p>Attracting and retaining talent</p>	 <p>Building a secure and trusted organisation</p>

Source: ADAPT CISO Edge, Digital Edge, CFO Edge, CIO Edge and Data Edge Surveys in 2022. Sample Size: 628 Australian Executives

3 Best Practice Three

Australian organisations will realise three main benefits by embedding security principles into their data-driven architectures. These benefits include:

1. Improved threat identification and defence

Security teams can leverage analytics to predict the impact of existing vulnerabilities or emerging risks.

This data-driven approach will offer real-time insights via behavioural analytics, intrusion detection, and allow the organisation to map its architecture against the changing nature of these risks.

These insights will and enable security teams to become more proactive.

2. Greater progress through evidence-based decision making

These insights will inform how executives prioritise investments that will safeguard the organisation, its people, and the data it holds.

It can also enable them to benchmark their progress against their competition, positioning the organisation for competitive advantage.

3. Security by design through a culture cultivated by executives and employees

Embedding security into data programs requires consistent culture and controls. Identify and ringfence sensitive data assets and access points.

Converse with data owners to culture of least privileged access and investigate a zero-trust model to manage the associated risks.

3 Best Practice Three

Actions for CISOs to build a safe and secure data driven strategy

To realise these outcomes, CISOs can:

- **Apply ADAPT's CIAD Model**, published in April 2021. This will involve designing a data architecture that secures the collection, integration, and analysis of data, always with the decisions and outcomes in mind.

Empower data scientists and machine learning experts to augment incident detection, prevention and response.

- **Educate technology teams, executives and business users** about the behaviours that will reduce the risks of confidential information being leaked.

Cultivating these safe and secure behaviours will lead to smarter investment decisions and enhance cyber readiness across the organisation.

The CISO of a financial services organisation described in an ADAPT Workshop Recording from November 2021:

“

The focus is how to use data to predict threats, get ahead of it and assign controls based on where they are going to be of best use.”

4 Best Practice Four

Review your specific vulnerability portfolio to create an adaptive defence framework

According to the *ADAPT Market Trends* report referenced earlier, 85% of Australian organisations say their ability to deal with threats improved in the 12 months to April 2022.

However, this is largely due to a few top performers, rather than deliberate design and planning.

These heroics of a few are not scalable.

It requires the security function's most skilled—and already overburdened—people to manually defend a changing, often invisible, perimeter.

It risks further fatigue that will lead to staff turnover.

Organisational Security – Maturity and impact

Maturity assessment

Disagree
 Neutral
 Agree

Ability to deal with security threats improved in the last year



Security is built into new systems from the start of projects



Security features are included in project planning time



It is difficult to tie security spend to business outcomes



The security team is perceived as an inhibitor



Impact assessment

Decrease >10%
 Marginal Change
 Increase >10%

Security team workloads



Need for security awareness and training



Focus on cyber security strategy refresh



Third-party risk exposure



Number of security incidents



Source : ADAPT CISO Survey August 2021 & CISO Edge April 2022 172 CISOs and Heads of Security

4 Best Practice Four

ADAPT also surveyed 160 CISOs to determine the top five threats they are most concerned about:

1. Ransomware 
2. Data security 
3. Phishing and socially engineered attacks 
4. Third party risks 
5. Cloud security 

These threats fundamentally revolve around data, people, and technology architecture.

By contemplating these threats in planning, design and technology enablement, CISOs can develop a greater understanding of their specific vulnerability portfolios and act accordingly.



4 Best Practice Four

Actions to review your vulnerability portfolio and develop an adaptive defence framework for defence

These actions will help CISOs to identify their specific vulnerabilities, prepare appropriate strategies across people and process, and defend the organisation through the most effective toolset.

- **Map the organisation's architecture** against the threat landscape. Use this mapping to assess your specific vulnerability portfolio.

Measure outcomes like process hardening, individual awareness of security and business maturity against regulations.

- **Assess cyber intelligence** coverage, integration and simplicity of toolchains, adoption of secure practices and efficacy of incident detection.

- **Shortlist effective technologies** to combat your specific vulnerabilities portfolio. Review the *ADAPT Expert Presentation* published in November 2022 to determine your prioritised roadmap.

Highly effective technologies include multi-factor authentication, endpoint security, and SIEM.

By developing an adaptive defence framework based on your specific vulnerability portfolio, CISOs can improve alignment with organisational policy, external regulations and prioritise the investments that will minimise risks.

Improving alignment—with engagement rather than compliance—is described in an *ADAPT Market Trends report* published in April 2022. In that report, Ansvar IT Manager Heather Santin advised:

“

It's not just about ticking the box of compliance. It really is about finding the high-risk areas and constantly monitoring [this] environment for safety.”

5 Best Practice Five

Ensure the interoperability of people, process and technology with security at its core

As described in the *ADAPT Persona Mapping report* referenced earlier, only 45% of organisations plan and design for security at the beginning of their IT initiatives.

Connected with these planning issues, only 33% said they have the optimal number of security tools; 37% are struggling with the burden of outdated or disconnected tooling.

These toolchain and planning issues are compounding the workload challenges faced by CISOs and their staff.

To what extent do you agree or disagree with the following statements?

■ Disagree ■ Neutral ■ Agree

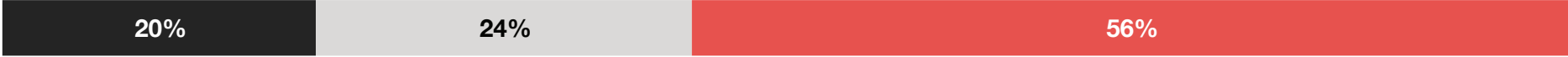
Our ability to deal with security threats has improved in the last year



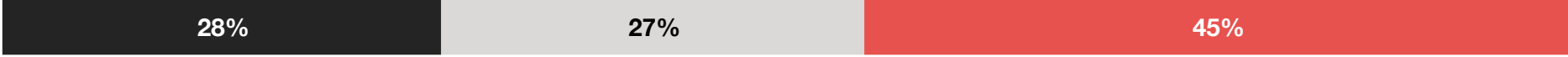
I find it easy to get senior management to understand security



Security is built into new systems from the start of projects



Security features are included in project planning time



We have too many security tools



Source : ADAPT CISO Survey August 2021 & CISO Edge April 2022 172 CISOs and Heads of Security

5 Best Practice Five

These toolchain and planning difficulties makes it harder to deal with an already complex threat landscape, and improper integrations may render these controls ineffective and create additional risks to the business.

As an example, threat monitoring data generated by these systems are often invisible to business users. This lack of transparency makes it difficult to assess and prioritise changes.

Actions that will facilitate interoperability across people, process and tools

- **Communicate the real risks**
which arise due to lack of interoperability between different systems with senior leadership and business users.
Place a dollar value on these risks.

- **Advocate for the strategic integration**
of security into planning and design. This will involve articulating the savings available from this approach, rather than bolting on security at the end.
- **Improve vendor evaluation frameworks**
to include security outcomes in your purchasing decisions.

For example, assess vendors on their ability to exchange information in a compliant way and review these decisions based upon open standards for security interoperability.

5 Best Practice Five

These actions will bring changes in the way security IT is bought, consumed and how it matures the organisation's cyber posture.

It will reduce the time-to-value of security investments, improve visibility into business risks, and improve decision making across the organisation's operating architecture.

Maturing the organisation's cyber posture through architectural design is described in an ADAPT Community Interview published in April 2022.

In this interview, Transgrid's Chief Security Officer Andrew Webster says that:

Architecture is the basis of all your good decisions. When architecting you need to be safe and secure by design.

Executive Actions



Australian businesses recognise the imperative to build a secure and trusted organisation, where those ambitions will be underpinned by the right culture and interoperability (technical, business) in the use and safe handling of data.

CISOs should use ADAPT's five practices to enable these changes and safeguard business value:

1. Engage with stakeholders to demonstrate the value of secure change.
2. Assess skills and cultural gaps to build the right IT and business competencies.
3. Build a data-driven organisation through safe and secure behaviours.
4. Review your specific vulnerabilities portfolio to create an adaptive defence framework.
5. Ensure the interoperability of people, process and technology with security at its core.

With these practices, CISOs can develop skilled employees, deploy technologies and change security mindsets to maintain organisational resilience. To discuss these best practices as they relate to your organisational context, please contact your customer success manager.

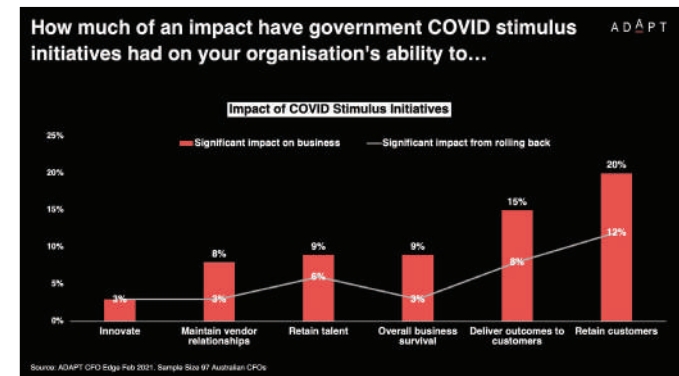
RESEARCH & ADVISORY

Australia's #1 source of local market insights, fact-based research & industry data

The Australian market is both unique in its dynamics and characteristics.

The challenge is often distilling the right global information to apply locally for effective strategic decision making. That's why ADAPT's Research & Advisory practice focuses exclusively on Australia and New Zealand market data.

Our dedication to local-first insights means you gain unrivalled access to in-depth Australian research, downloadable data and local peer case studies.



ADAPT's Research & Advisory services enable you to...

- ✓ **Validate strategies and plans** to maximise successful execution of projects and initiatives.
- ✓ **Stay up-to-date with local trends** and access best practice insights from global thought-leaders.
- ✓ **Gain stakeholder buy-in and trust** with a deeper understanding of key priorities being faced by ANZ executives.
- ✓ **Accelerate decision making** and save time conducting manual research.
- ✓ **Build robust business cases** using data/stats direct from ANZ technology and business community.
- ✓ **Learn the best practices of local executives** and gain insights into their key initiatives and business projects.

To learn more visit

adapt.com.au/research