White paper

Innovation over cybersecurity:

The contradiction within Australian business

rackspace®

aws partner network

Premier Consulting Partner

1. Introduction – Innovation or cybersecurity?

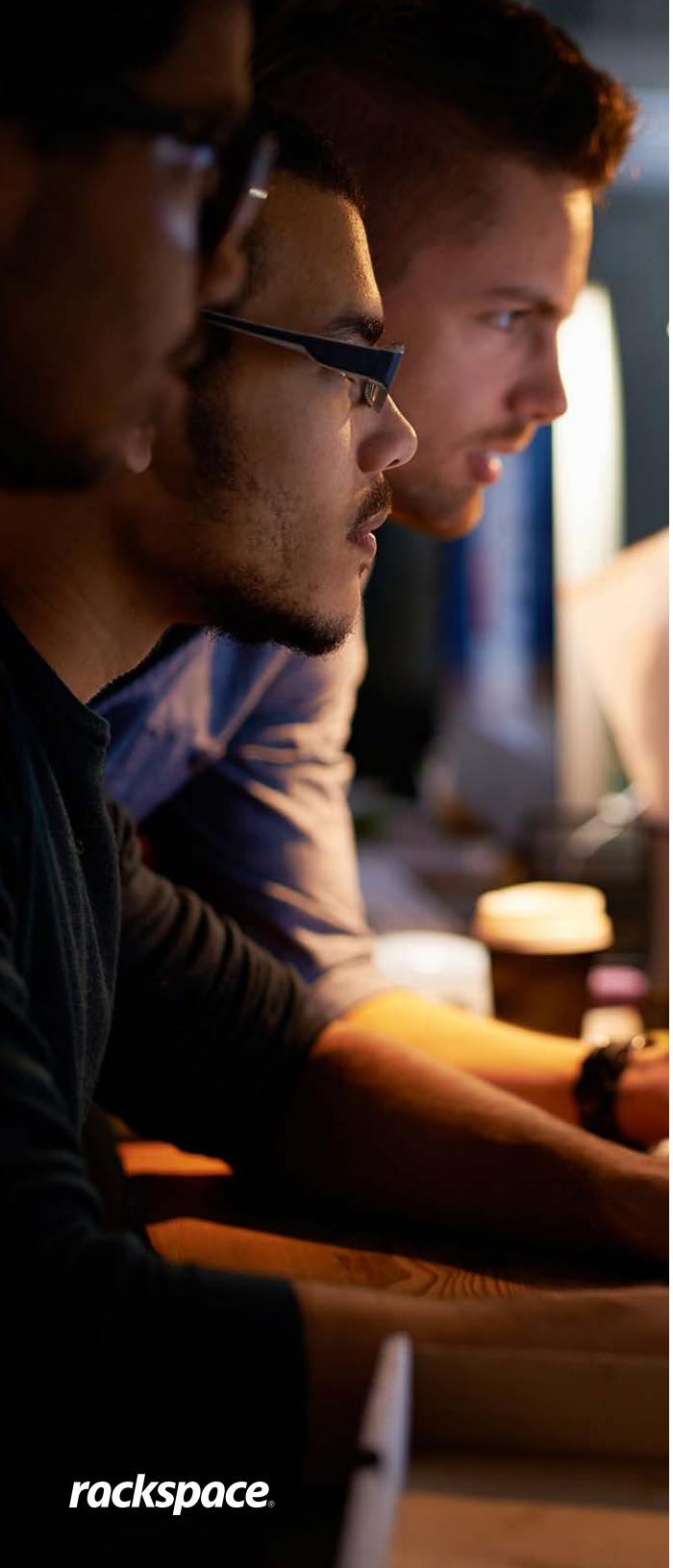
New research into cyber risk and digital transformation shows that Australian organisations place the highest importance on improving employee productivity, as well as enhancing business resilience. **Yet there is a conflict**. Enabling staff and third parties to access data off-site is the greatest threat to organisations from a cyber-security perspective. These concerns are further compounded by a lack of confidence in their capabilities to manage these risks.

The research uncovered tension between what organisations seek to achieve through their digital transformation efforts, their concerns about the risks created by their ambitions, and how well placed they are to solve them.

Given the importance organisations place on digitisation to transform operations, resolving this tension is critical to their businesses' long-term success.

Business leaders can start to address this conflict by asking themselves: "How do we confidently manage the cyber risks inherent in our digital strategy?"

Armed with the insights from this research, CIOs need to lead this discussion. The findings offer the perfect opportunity to elevate the cyber security discussion and deliver lasting value through strategic security programs tightly aligned to corporate ambitions.



2. Organisations focus transformation projects on the fundamentals

Our research found the majority of organisations placed more importance on digital transformation projects to improve the way their organisations operate with three-quarters of respondents rating 'improving employee productivity' and 71 per cent rating 'improving business resilience' as highly or extremely important for their digital ambitions.

What do organisations want to achieve?

Percentage of respondents rating the following factors highly or extremely important for their digital ambitions

1. Improve staff productivity — 75%
2. Enhance business resilience — 71%
3. Increase organisational agility — 69%
4. Improve customer experience — 66%
5. Develop innovative products and services — 63%

The research shows that ensuring core functions and staff are operating optimally is likely an enabler for employees to experiment with innovative solutions or new customer experiences. In this sense, operational benefits and business agility are the vital foundations for more transformative innovation.

However, when evaluated against respondents' views on cyber risk (in the next section), this desire for more productivity, resilience and agility is tempered with their concerns about their control over data.

3. Cyber risks: Data Control is a Priority

Too often, security is viewed as a barrier for transformation initiatives. Research[1] shows that cyber security issues are still seen as holding back innovation. They are a barrier, not part of the strategic conversation.

In a 2015 study of IT decision makers by BT, almost half (49 per cent) admitted they were 'very or extremely anxious' about the security implications of cloud services. With only 30 per cent of respondents in our research considering public cloud to be a significant risk, acceptance is clearly growing as public cloud platforms mature, regardless of the size of the organisation.

How much risk does this expose organisations to?

Percentage of respondents rating the following factors highly or extremely risky to their organisation:

1. Sharing data with third parties, allowing them to access your systems — 43%
2. Enabling staff to access data, anywhere and anytime — 34%
3. Using public cloud platforms — 33%
4. Using multiple, disparate cloud services for 'the right application in the right environment' — 33%

Despite their desire for greater staff productivity, or perhaps because of it, over one-third of respondents rated 'enabling staff access to data anytime and anywhere' as posing a high or extremely high risk to their organisation. Respondents also rated 'data sharing with third parties' as the most concerning risk area for their organisation (43 per cent rated this 8 or higher for risk).

[1] In 2017 Webroot and data centre organisation IO commissioned a survey of 500 senior decision makers from UK businesses of varying sizes. It found that 80 per cent of respondents believed security issues were impeding innovation. As well as this, 57 per cent thought that hasty innovation would compromise security. Source: Disruption

Their concern about data is also reflected in the respondents' view on the potential effect of cyber breaches. Data loss ranked top for its potential effect on a business (86 per cent rated it 8 or higher for impact on their organisation). This outweighed lost revenue (67 per cent). Understandable, as data loss can lead to reputation damage, regulatory action, loss of customer trust or direct financial loss through ransomware.

What is the perceived impact on organisations?

Percentage of respondents rating the potential impact of these factors as highly important to their organisation:

1. Loss of data — 86%
2. Business interruption — 81%
3. Reputation harm — 76%
4. Loss of revenue — 67%
5. Regulatory action — 67%

When viewed against businesses' objectives, there is a tension. Businesses want to empower their teams to work wherever they need to, whenever they need to. Over three-quarters of respondents rated this as a highly important factor in their business's ability to achieve the benefits of digital transformation.

Organisations also want to enhance resilience and maximise value from their data. On-premises servers might be more secure but they can be limiting. All of this requires a more flexible approach to data access.

This demand is likely to become even more important as more businesses adopt artificial intelligence (AI) applications. AI requires large data sets and significant compute power. Many companies will access these applications through third-party, cloud service providers. Deloitte says that "*among companies that adopt AI technology, 70 per cent will obtain AI capabilities through cloud-based enterprise software, and 65 per cent will create AI applications using cloud-based development services.*"

4. Capabilities for Control

Organisations want to be confident they have control and visibility over their data.

Respondents rated security tools, skilled staff, and visibility of their data as the three most important factors for minimising cyber security risk.

Partnerships with skilled vendors followed close behind, reiterating the value of cloud security skills in today's increasingly risk-sensitive world.

What capabilities do organisations value?

Percentage of respondents rating the following factors as highly important for minimising cyber security related risk:

1. Security tools[2] — 77%
2. Staff with the right skills who are available when you need them — 74%
3. Data visibility — 68%
4. Partners with the right skills, available when you need them — 67%
5. Reporting tools and insights — 66%
6. Connectedness between cloud and on-premises environments, staff, sites and partners — 63%
7. Cloud environments — 60%

While the tools and technology to manage risk are available, the talent requirement is more problematic. Cyber security skills are in high demand and expensive. In Australia, AustCyber's 2018 security sector competitiveness plan estimates a persistent cyber skills shortage equating to a shortfall of 2,300 workers.

This throws the importance of partners into sharp relief. Organisations are unlikely to get the skills they need in-house (and keep them) in such a competitive market. Partners offer a valuable way of accessing those skills.

Given the perceived risk of data loss and the importance of data control, data visibility rated highly as a capability that organisations need to minimise cyber risk. And here skills play an important role too. Especially in architecting hybrid or multi-cloud deployments. Data is often fragmented across organisational silos, server locations and cloud platforms.

Fragmentation makes it harder for organisations to protect data. It also makes it harder to realise the benefits of data. Seventy-one per cent of respondents rated data visibility as highly, or extremely important for the organisation to achieve the benefits of digital transformation.

There is another angle to the skills question, one that applies to the whole business. The human factor is often an organisation's greatest vulnerability. Phishing and ransomware are targeted at individuals to circumvent security controls. Regular effective training programs and a 'whole of business' security mentality are important for minimising cyber risks.

[2] Security tools may include:
1. Firewall
2. Anti-virus software
3. PKI Services
4. Managed detection services
5. Risk assessment
5. Penetration tools
6. Staff training

5. A Capability Gap

The importance Australian organisations place on tools, skills and data visibility is clear. But confidence in their capabilities in these areas is more nuanced.

Fifty-six per cent of respondents stated they were highly confident their organisation had the security tools to minimise cyber security risk and deliver digital transformation goals. However, only half of all respondents were highly confident they had access to the right skills.

How confident are organisations they have the right capabilities?

Percentage of respondents who are highly confident that their organisation has the following capabilities:

1. Security tools[2] — 56%
2. Staff with the right skills who are available when you need them — 50%
3. Data visibility — 48%
4. Partners with the right skills, available when you need them — 50%
5. Reporting tools and insights — 47%
6. Cloud environments — 54%
7. Connectedness between cloud and on-premises environments, staff, sites and partners — 44%

Larger organisations tend to be more confident in their capabilities than SMEs. Possibly because they can dedicate more resources to cyber security and recruit the right talent. However, nearly half of respondents from these organisations were not highly confident their organisations had access to the right skills to manage their risks.

A lack of confidence in cyber security capabilities can directly influence an organisation's appetite to incur risks as part of their digital transformation strategy.

Greater confidence can encourage organisations to pursue more radical change that delivers increased business benefits. Conversely, uncertainty can shape the direction of digital transformation projects from the very beginning. This often limits their impact or impedes the progress of innovation.

[2] Security tools may include:
1. Firewall
2. Anti-virus software
3. PKI Services
4. Managed detection services
5. Risk assessment
5. Penetration tools
6. Staff training

6. Conclusion – Three Actions for Organisations

a. Treat growth, innovation and security as one conversation.

Cyber security should be considered within the wider transformation agenda (and vice versa) from the beginning. Then it can be a true value-generator rather than a cost base. Conversely, treating them separately only serves to hinder digital transformation outcomes, or increase organisations' cyber risk.

This requires CIOs, CISOs, CEOs and other functional leaders to develop a shared understanding early on, of what the organisation is trying to achieve. They also need a clear view of the potential risks, and an honest assessment of their capabilities.

Organisations can then prioritise investment in the cyber capabilities that will have the greatest effect in helping to deliver the business' ambitions.

b. Consider how you will win the war for talent

Access to the right skills is vital to the success of cyber security programs. Organisations should take a strategic approach. Begin by identifying the skills you need. Evaluate your digital ambitions and the likely risks that such a program may create. Then, consider whether it makes more business sense to invest in finding and bringing in the level of talent you require to improve your organisations' capabilities. Alternatively, seek a specialist partner that can offer the right skills and tools.

c. Adopt DevSecOps

DevSecOps is a way of working that introduces security earlier in application development. It minimises vulnerabilities, brings security closer to IT and business objectives, enabling rapid application iteration while remaining secure.

As more organisations come to see the value of security in their innovation agenda, DevSecOps may become a critical competitive advantage in the way that agile working is now. Gartner estimates DevSecOps will be embedded into 80 per cent of rapid development teams by 2021.

A Final Word

Organisations should view cyber security capabilities as a foundation upon which they can move forward confidently to transform their operations, products and services.

As Stephane Nappo, Global Chief Information Security Officer at Société Générale International Banking, and 2018 Global CISO of the year, said: *"Security must reinvent itself to properly support our innovative ecosystem".*

Successfully aligning cyber security investments with the business' innovation objectives helps organisations become less risk averse and more risk confident. It supports transformation and creates a lasting competitive advantage.

rackspace.com.au

Appendix – Methodology

AMR conducted the research on behalf of Rackspace and sponsored by AWS. AMR surveyed 202 Australian business executives with influence in their organisation's cloud technology decision-making. Respondents were drawn from businesses of all sizes, with half representing organisations with over 500 employees.

rackspace.

aws partner network

Premier Consulting Partner

About Rackspace

At Rackspace, we accelerate the value of the cloud during every phase of digital transformation. By managing apps, data, security and multiple clouds, we are the best choice to help customers get to the cloud, innovate with new technologies and maximise their IT investments. As a recognised Gartner Magic Quadrant leader, we are uniquely positioned to close the gap between the complex reality of today and the promise of tomorrow. Passionate about customer success, we provide unbiased expertise, based on proven results, across all the leading technologies. And across every interaction worldwide, we deliver Fanatical Experience™ — the best customer service experience in the industry. Rackspace has been honoured in the top 20 Great Places to Work Australia for the past 7 years. Learn more at rackspace.com.au.

About AWS

For over 12 years, Amazon Web Services has been the world's most comprehensive and broadly adopted cloud platform. AWS offers over 165 fully featured services for compute, storage, databases, networking, analytics, robotics, machine learning and artificial intelligence (AI), Internet of Things (IoT), mobile, security, hybrid, virtual and augmented reality (VR and AR), media, and application development, deployment, and management from 60 Availability Zones (AZs) within 20 geographic regions, spanning the U.S., Australia, Brazil, Canada, China, France, Germany, India, Ireland, Japan, Korea, Singapore, Sweden, and the UK. AWS services are trusted by millions of active customers around the world—including the fastest-growing startups, largest enterprises, and leading government agencies—to power their infrastructure, make them more agile, and lower costs. To learn more about AWS, visit aws.amazon.com.