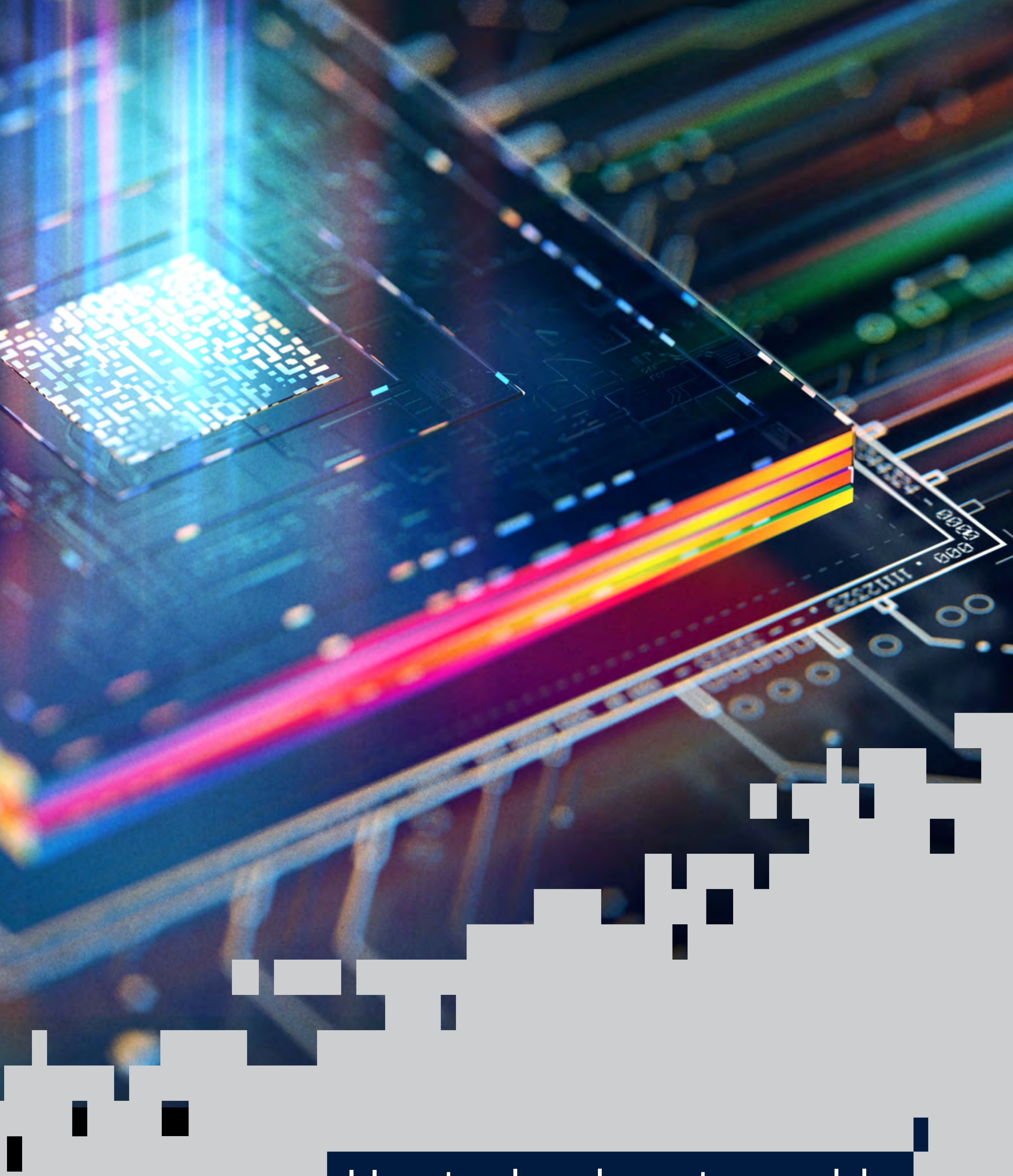
RSM

Cyber storm rising:

Navigating the path to resilience for Australian business

THE POWER OF BEING UNDERSTOOD
ASSURANCE | TAX | CONSULTING



Use technology to enable operational excellence

Introduction

The escalating frequency, sophistication and cost of cyber threats have made cyber resilience a critical concern for businesses. IBM's Cost of a Data Breach Report 2024 shows the average cost of a cyber attack to an Australian business is $4.17 m[1] (US$2.78 m), up from $4.05 m (US$2.7 m) in 2023. Equally as concerning, the Australian Signals Directorate's (ASD) figures indicate Australian businesses are hit by a cyber attack every six minutes[2].

Average cost of a cyber attack to an Australian business is

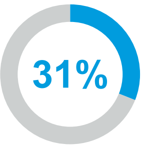
$4.17 m

Australian businesses are hit by a cyber attack every

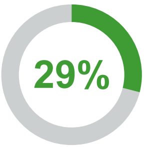
6 minutes

RSM Australia surveyed 150 Australian business leaders in July 2024 and the findings, along with analysis from RSM's cyber specialists and other industry experts, inform this report, *Cyber storm rising: navigating the path to resilience for Australian business*.

RSM Australia's report shows just under a third (31%) of Australian businesses are not prepared to face, let alone recover from, a serious cyber incident. At the same time, this is an environment in which 29% of large organisations have experienced one or more cyber attacks in the past 12 months.



Australian businesses **are not prepared** to face a serious cyber incident



Large organisations have **experienced one or more cyber attacks in the past 12 months.**

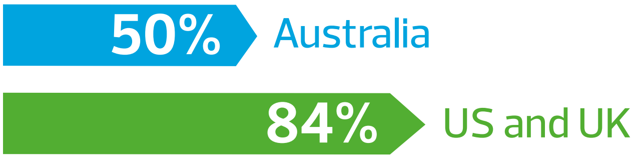
This is especially concerning with the advent of the Australian Prudential Regulation Authority's upcoming prudential standard, CPS 230 Operational Risk Management, which comes into force in July 2025.

While targeted at financial services, the standard puts the onus on Australian businesses to establish an information security capability that ensures the confidentiality, integrity and availability of information assets.

Against this backdrop, RSM Australia has undertaken extensive research to understand how leaders within Australian businesses are approaching cyber security, to assist organisations to better understand the threat environment and develop best practice mitigation strategies.

This report is part of a global series of research and thought leadership pieces by RSM that assess business leaders' perceptions of cyber security and readiness to combat rising cyber risks. The Australian study follows similar research that has been conducted by RSM UK and RSM US.

Drawing on extensive interviews with senior leaders across Australian businesses, the data shows a worrying lack of preparedness to face serious cyber threats, especially when compared to their overseas counterparts. Only 50% of respondents said they are **confident in their staff's capacity to manage cyber security risk**. This compares with 84% of US and UK firms that have confidence in their organisation's ability to manage cyber risks.



[1] Cost of data breach report 2024, IBM, August 2024

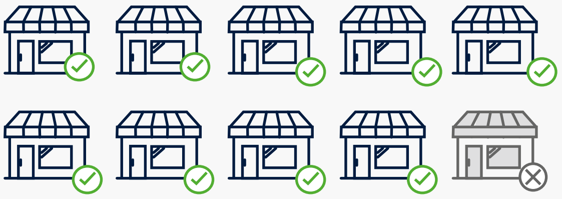
[2] ASD Cyber Threat Report 2022–2023

For Australian firms to improve their cyber security posture, they urgently need to invest in risk management, tailored security measures, regular testing and foster a culture of resilience across their operations. It's essential boards of directors, senior management teams, IT and security experts in organisations immediately embed systems, processes and policies to achieve continuous improvement in managing their cyber risks, or face serious negative financial and reputational consequences.

The report consequently outlines a strategic approach businesses can follow to ensure their cyber security capabilities are commensurate with the scale and nature of potential threats.

As this study shows, in the wake of high-profile cyber incidents, the need for robust cyber resilience must be a top priority for all Australian organisations.

While almost nine in 10 (89%) large organisations and 65% of mid-sized organisations have increased their investment in cyber security in the past 12 months, more needs to be done, and across the spectrum of large, medium and small organisations, to decrease the risk and consequences of attack.



Almost nine in 10 organisations have increased their investment in cyber security in the past 12 months

Exploring the risk landscape

Cyber security is an ever-evolving landscape, where cyber criminals proliferate and new technologies such as artificial intelligence (AI), the Internet of Things and cloud services expose organisations to new and potentially catastrophic risks. According to the ASD, it received more than 94,000 cybercrime reports over the 2022/2023 financial year .

Some of the most serious risks Australian businesses face include:

- Significant financial impacts, particularly in relation to ransomware attacks.
- Paralysing data security breaches, where data leaks can incapacitate an organisation, sometimes for months at a time, destroying corporate reputations and consumer and shareholder trust.
- Serious regulatory non-compliance, leading to penalties of up to $50 million for privacy breaches .

To fully understand the threats they face, organisations must appreciate cyber criminals are increasingly using very sophisticated programs to scan their internet-facing networks to identify vulnerabilities.

This smart scanning is becoming even more successful thanks to criminals use of machine learning and artificial intelligence to infiltrate large Australian businesses' systems and networks.

As a result, cyber criminals can be more selective about who or what they target, because they are more easily able to identify low hanging fruit.

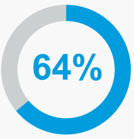
Criminals are also operating with more stealth. They once had to spend much more time in a business system than they need to today. This is because now, once they are in a business system, they are able to almost instantly learn about vulnerabilities and where sensitive information is held. So, it has never been more important for organisations to understand the cyber threats they face, the weaknesses within their IT networks and across their operations and ways to mitigate risks.

Key findings

RSM Australia surveyed 150 Australian business leaders in July 2024 to determine awareness of cyber security risks and preparedness in Australia.

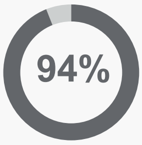
Australian businesses, especially large ones, are readying themselves to face cyber threats.

However, they need to improve their cyber security. The research shows 31% of Australian businesses are unprepared or very unprepared to face a cyber attack. But almost half of large organisations have done no internal testing and more than half have not tested their wifi or web applications or done external testing, which means they are extremely vulnerable to attack.



Australia

Australian businesses say they feel prepared to respond to a cyber attack

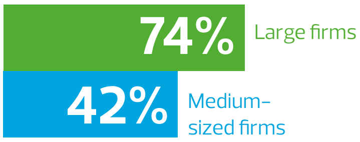


UK/US

US and UK businesses are ready to respond to a cyber attack

Australian leaders' confidence in managing cyber risks is lower than their US and UK counterparts, suggesting a need for more training and investment in this area. Only half the respondents surveyed said they have mid to high levels of confidence in their staff's capacity and capability to manage cyber security risk. This is significantly lower than the UK/US figure of 84%.

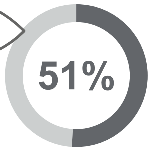
Vulnerability testing is not widely practised, with less than half
41% of businesses conducting tests annually, despite their importance in identifying security issues. The results show just 66% of large organisations have run a response test to a cyber attack in the last 12 months, with this figure being 55% for mid-size firms.



While larger businesses are closer to global averages in cyber insurance adoption, there's still a need for better protection against cyber incidents. In total
74 % of large firms have cyber insurance, the same percentage as the US/UK. But only 42% of medium-sized firms have cyber insurance while 20% of large business respondents were unsure if they have cyber insurance and 6% did not have any cyber insurance.

Phishing remains the prevalent cyber threat and it needs to be better managed in terms of damage control and resource allocation. A total of 46% of large organisations have experienced a successful phishing attempt. Worryingly, 42% of firms' existing security response plans were unsuccessful in limiting the damage related to direct data extraction, which is often the result of a phishing attempt, with 27% of firms taking more than a month to recover from ransomware and extortion, with 40% of firms taking between a week and a month to recover.

Australian medium-sized businesses are particularly vulnerable to third-party data breaches.
In total 32% of businesses have had a third-party data breach in the last 12 months, with this figure rising to 42% of medium-sized businesses.

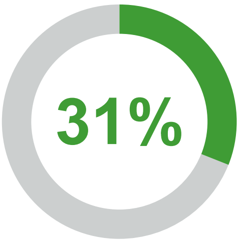


The future focus is on AI-enabled attacks, with 51% of businesses making protecting against AI enabled cyber attacks, their top priority. Protecting against ransomware and extortion attacks are a close second, mirroring results in the US and UK.

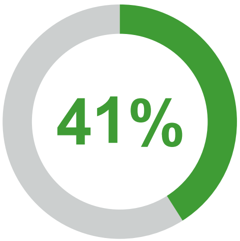
Results

How prepared are Australian businesses to respond to a cyber attack?

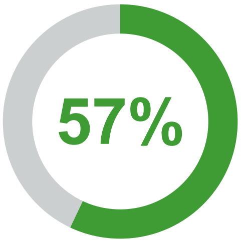
Australian businesses need to be much better prepared to anticipate and thwart cyber attacks.



31% of Australian businesses **are unprepared or very unprepared to face a cyber attack.**



41% of all organisations have **never run a response test to a cyber attack.**



Only 57% of large organisations **have internally tested their response to a potential cyber attack.**

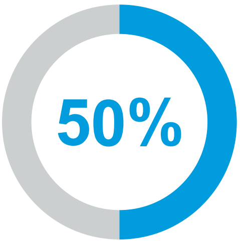
Expert Opinion

There is an urgent need for firms to look at their cyber security culture and cyber risk preparedness to ensure they are ready for the next major glitch, outage or attack.

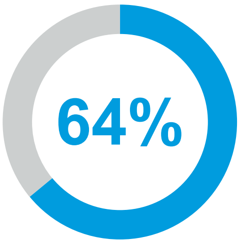
"It is critically important for organisations to conduct thorough and regular risk assessments to identify vulnerabilities and potential threats," says Ashwin Pal, Partner, Security and Privacy, RSM Australia.

How confident are Australian leaders to manage cyber risks?

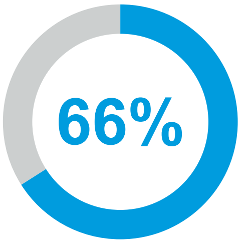
Australian leaders' confidence in managing cyber risks is lower than their US and UK counterparts.



50% of respondents say they have mid to high levels of confidence in their staff's capacity to manage cyber security risk, versus 84% in the UK.



64% of Australian businesses say they feel prepared to respond to a cyber attack, versus 94% in the UK.



66% of large organisations have run a response test to a cyber attack in the last 12 months.

Expert Opinion

As the research shows, it's concerning Australian entities are currently lagging their counterparts in the US and UK in terms of cyber resilience.

"This gap presents a significant opportunity for local firms to enhance their cyber defences," says Darren Booth, Partner, Security & Privacy, RSM Australia.

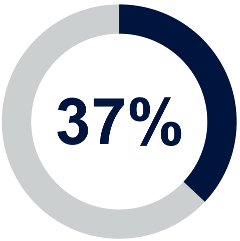
To address this gap, businesses must invest in training, hire cyber security professionals and adopt best practices so they have the same level of cyber resilience as their international counterparts.

Importantly, says Riaan Bronkhorst, Partner, Security and Privacy, RSM Australia, regular testing is essential for identifying and fixing gaps in incident response and business continuity plans.

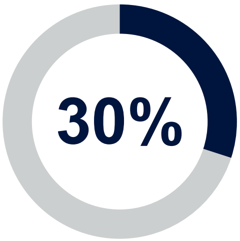
"Without rigorous testing, organisations may overestimate their level of prep aredness, leading to disastrous outcomes during actual cyber incidents," he says.

How prepared are Australian businesses to respond to a cyber attack?

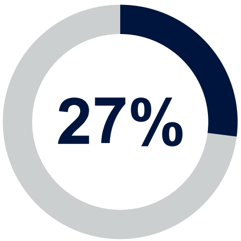
For around one in three firms, it is taking more than a month to recover from cyber attacks/incidents.



37% of firms are taking **more than a month to recover from data leaks.**



30% of firms are taking more than a month to **recover from data exfiltration due to a supplier being compromised**



27% of firms are taking **more than a month to recover from ransomware and extortion.**

Expert Opinion

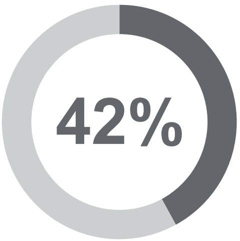
"Businesses should define and regularly do internal and external vulnerability assessments and security testing to identify any weaknesses and ensure that they maintain a robust security posture to defend against potential cyber threats," says Riaan Bronkhorst, Partner, Security & Privacy, RSM Australia.

Businesses must prioritise cyber security testing, including:

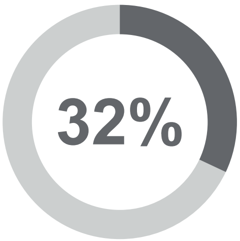
- Performing vulnerability assessments.
- Holding incident response drills.
- Conducting business continuity planning exercises.

What risk do third-party data breaches pose to Australian businesses?

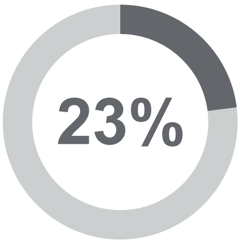
Third-party data breaches are a risk to Australian business.



42% experienced a **third-party data breach in the last 12 months.**



32% of all businesses **have had a third-party data breach** in the last 12 months.



23% of these **experienced a financial, reputational or operational impact** as a result of a third-party data breach.

Expert Opinion

When it comes to assessing third parties' level of cyber security, what's key is a high level of professional scepticism.

"Businesses need to do thorough due diligence around who their supplies are, how they would survive without them and what happens if they are the involved in a major cyber security event," says Ashwin Pal, Partner, Security and Privacy, RSM Australia.

It's vital to have a methodical and structured approach to managing third party cyber risks."

What are the main cyber threats businesses face?

The top threat to businesses is the constantly evolving threat landscape. Businesses say their top three cyber risks are:

1

The constantly evolving threat landscape.

2

The complexity of their IT infrastructure.

3

Lack of staff compliance and insufficient staffing and training.

Expert Opinion

A culture of resilience is crucial for proactive cyber risk management.

"Many businesses still operate with a mindset of apathy or complacency, which can be detrimental in the face of evolving cyber threats," warns Darren Booth, Partner, Security & Privacy, RSM Australia.

Fostering a culture of resilience requires a shift in mindset at all levels of the organisation. This includes regular training and awareness programs, clear communication of cyber risks, and incentivising proactive cyber risk management behaviour through KPIs and performance metrics. "Leaders must set the tone by demonstrating a commitment to cyber resilience," Booth adds.

While board members may not be technical experts, they play a critical role in overseeing the organisation's risk management process.

"Engaging the board in cyber risk discussions is essential to ensure the organisation's cyber resilience strategies align with its overall risk appetite and governance framework," says Ashwin Pal.

Ultimately, it's the board's responsibility to mitigate cyber risks. They should be involved in understanding and approving cyber security initiatives, with regular and accurate reporting to them so they know what progress has been made in improving the business's cyber security posture. The board's engagement should be structured to provide strategic guidance and oversight without micromanaging technical details.

Stephen Gillies, Technology Evangelist APAC at edge cloud platform Fastly expects to see an increased acceleration of new attack vectors, a renewed focus on identifying the attack surface for globally provisioned applications and a next generation of cyber security issues.

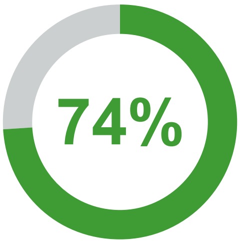
"Emerging new technologies in the Quantum cryptography space and the impact of an explosion of intelligent Internet of Things (IoT) devices connected to the global Internet will forever change how we deploy and protect our applications.

Today we're seeing the rapid adoption of AI tools and large language models (LLM) impact data compliance, the effectiveness of human security analysts, and the speed at which applications can be prodded and probed for bugs, security issues and availability. In some cases this is positive, allowing enterprises to test and build their applications more efficiently, but introduces the potential of copyright infringements, the potential use of substandard AI constructed code which results in an impact to innovation, and an eventual loss of 'programming elegance.

The road ahead will be challenging for businesses and governments alike, and while some organisations are doubling down on application audits and observability, if we're not skilling our teams with AI tooling we're already falling behind," says Gillies.

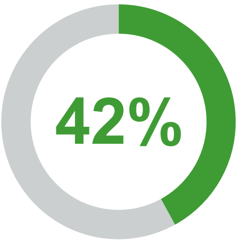
How many businesses have cyber insurance?

The majority of large businesses have cyber insurance but there is little uptake among the small business sector.



74% of large firms **have cyber insurance.**

20% of large business **respondents were unsure if they have cyber insurance.**



42% of medium-sized firms **have cyber insurance.**

Expert Opinion

Large business cyber insurance uptake is on par with global incidence rates. Large businesses feel prepared and are gearing up to respond to cyber threats but there is opportunity to improve. Colin Pausey, chief operating officer of specialist cyber insurer Emergence, explains third-party risks are more significant now than they ever have been because businesses' networks are more interconnected than ever before.

"You can have the best controls in the world and your processes can be let down by weaknesses in your third party supply chain. If they are not able to deliver goods and services, that impacts your business," says Pausey.

"You only have to look at the CrowdStrike outage in July 2024 to realise that even if there has been no system failure in your business, but there's been a system failure in one in your supply chain, it can have major consequences," he says.

Reducing this risk involves developing a deep understanding of the supply chain and asking pointed questions of suppliers.

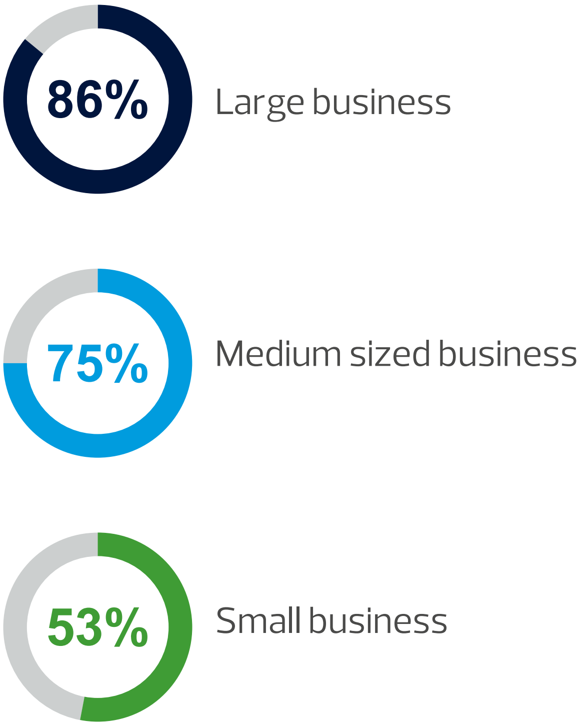
Pernille

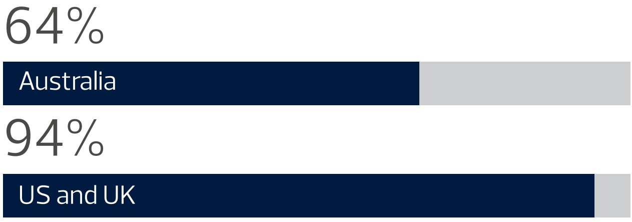
One of the RSM team

Understanding the data on cyber attack preparedness, incidences and mitigation

The research findings in this report reveal a concerning gap in the preparedness and capacity of Australian businesses, particularly small and medium-sized enterprises, to effectively anticipate and respond to cyber attacks. This highlights the need for significant improvements in cyber security measures across Australian businesses.

1 Australian businesses need to be much better prepared to anticipate and thwart cyber attacks





In total, 64% of Australian businesses say they feel prepared to respond to a cyber-attack. However, this figure is significantly lower than the US and UK, where 94% of businesses are ready to respond to a cyber attack.

⊗ ✓ ✓

Worryingly, almost one in three Australian businesses are unprepared to face a cyber attack.

These results indicate there is a significant opportunity, especially among small and mid-sized firms, to improve Australian business's skills, experience and capacity to manage cyber security risks.

2 Staff are not prepared to respond to a cyber threat

✓ ⊗ ⊗

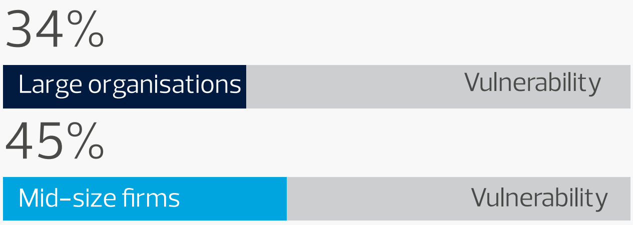
One in three large organisations are highly confident in their staff's ability

Larger organisations are more confident in their teams' capacity to respond to cyber threats than mid-sized and small organisations, although fewer than one in three large organisations are highly confident in their staff's ability to manage cyber security risks.

3 Fewer than half of all organisations have carried out vulnerability tests in the last 12 months.

More than a third of large organisations are extremely vulnerable because they have either never tested their response to a potential cyber attack or haven't done a test for more than 12 months.

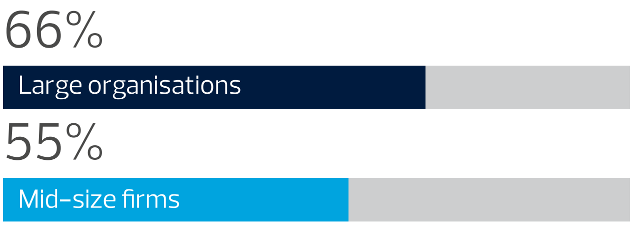
Vulnerability



The 45% of mid-size firms that have not run a vulnerability test for more than 12 months or that have never done a test are most vulnerable. The 34% of large firms that have never run a test or haven't run a test for 12 months are also vulnerable.

Response tests

41% of all organisations have never run a response test to a cyber attack.



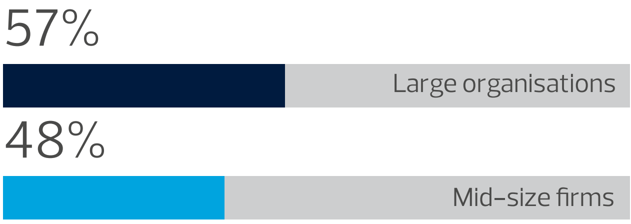
Larger organisations are much more likely to have run a response test than smaller organisations in the last 12 months.

4 External, internal, web and wifi tests are the most common vulnerability assessments undertaken across all organisations.

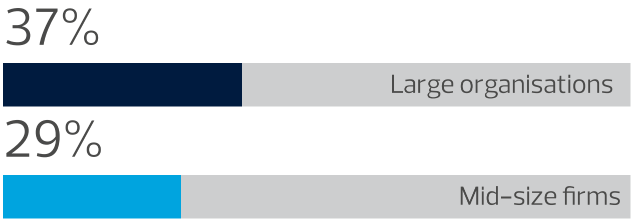
Large organisations are under-prepared to face a cyber attack. Almost half have done no internal testing and more than half have not tested their wifi or web applications or done external testing, which means they are extremely vulnerable to attack.

Mid-sized firms are even more under-prepared than their larger peers. Less than half of mid-sized firms have done internal testing, less than a quarter have done wifi testing and less than a third have done web application testing.

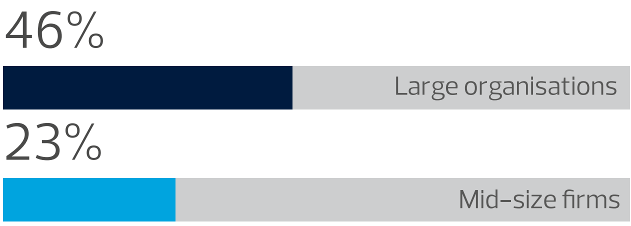
Internal testing



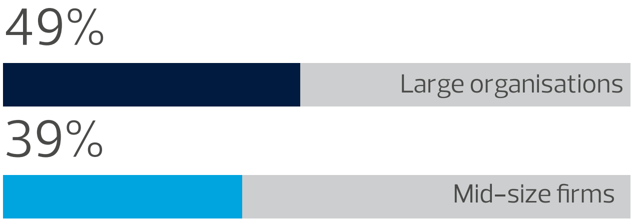
Web applications testing

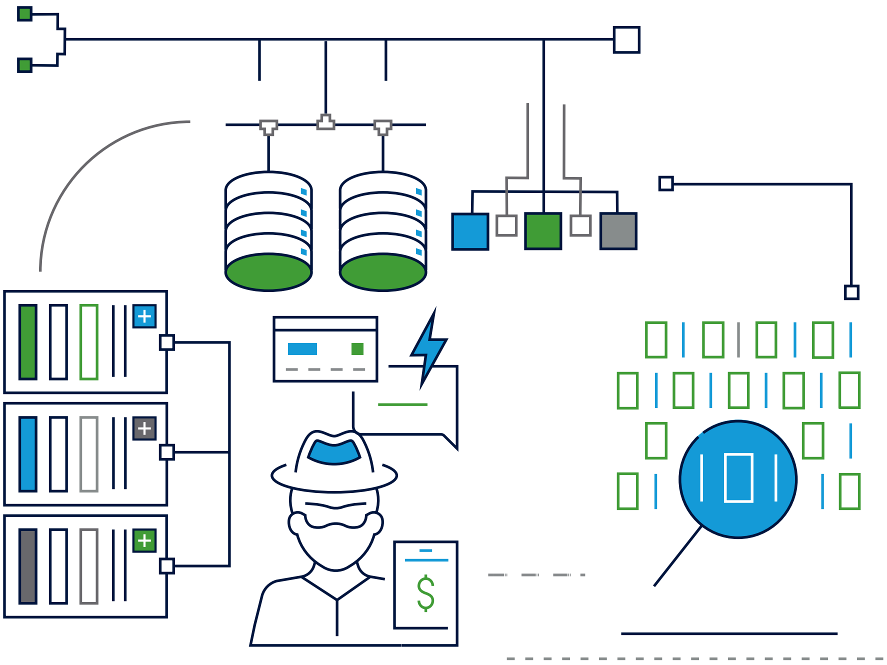


Wifi testing



External testing



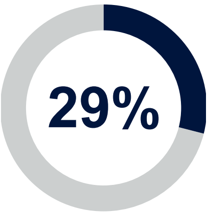


Kieran
One of the
RSM team
Empowering you to face
the future with confidence

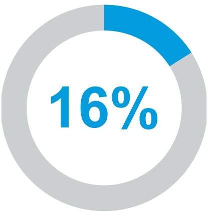
Cyber attack incidences and mitigation

1 Larger businesses are more likely to experience an attack versus small businesses

This shows how important it is for larger firms to improve their cyber security posture.

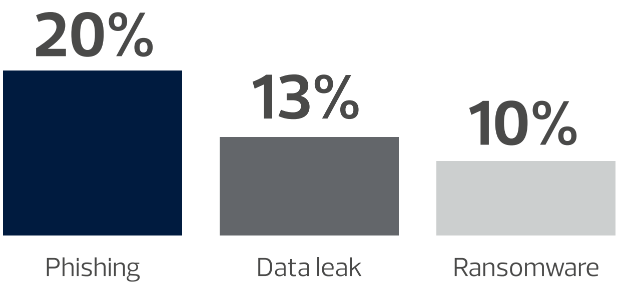


29% of large businesses have experienced one or more cyber attacks in the last 12 months.

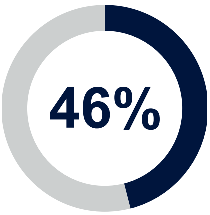


16% of mid-sized businesses have experienced one or more cyber attacks in the last 12 months.

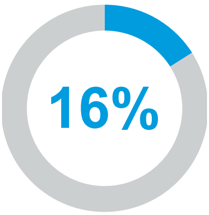
2 Damage limitation strategies are having only limited effects



Phishing is the most common form of attack, with 20% of all firms experiencing this type of attack, followed by data leaks at 13% and ransomware 10%. However recovery times are faster with phishing and longer with ransomware and data exfiltration (ie data stolen directly from systems).



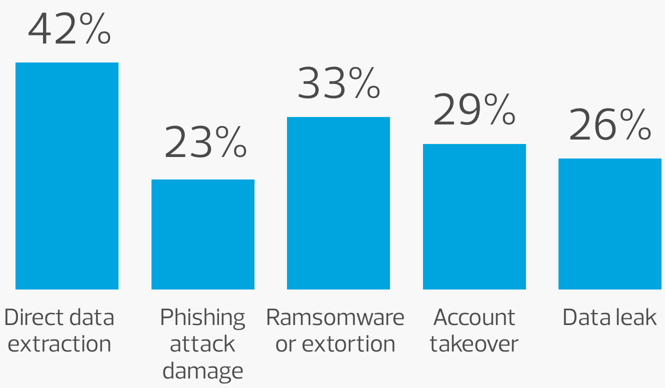
Large businesses



Mid-size businesses

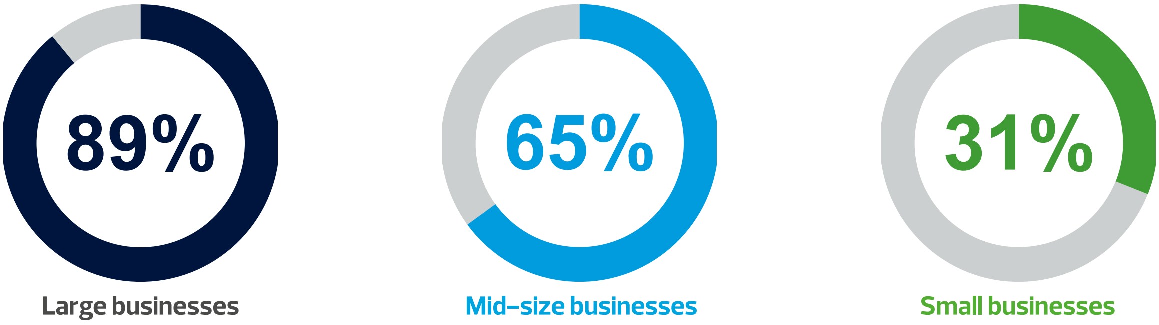
46% of large organisations have experienced a successful phishing attempt, with this figure dropping to 16% for mid-sized firms. Large organisations are more likely to have had a cyber attack. The trends are consistent with global indications, with phishing on the rise.

Security response



- Worryingly, 42% of firms' existing security response plans were unsuccessful in limiting the damage related to direct data extraction and 23% of firms' existing security response plans were unsuccessful in limiting the damage from a phishing attack
- 33% of firms' existing security response plans were unsuccessful in limiting the damage related to ransomware or extortion.
- 29% of firms' existing security response plans were unsuccessful in limiting the damage related to account takeover.
- 26% of firms' existing security response plans were unsuccessful in limiting the damage related to a data leak.

3 While preparedness needs to improve, firms are investing in their cyber security



Almost nine out of 10 (89%) of large organisations have increased their investment in cyber security in the last 12 months. This is significantly higher than mid-sized organisations, of which only 65% have increased their investment in cyber security over the same timeframe. Small organisations in particular are yet to respond to cyber security issues in a significant way, with only 31% taking action.

63%

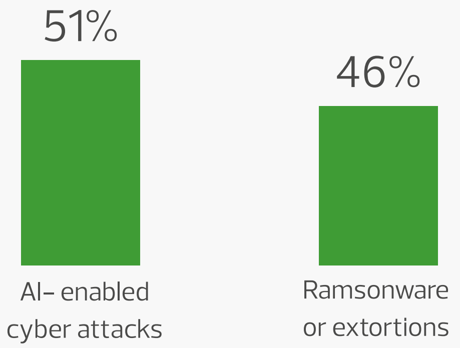
63% of large organisations have updated their policies and procedures over the last six months.

51%

51% of large organisations have recruited cyber security staff.

49%

49% of large organisations have engaged cyber security consultants to advise on strategy.



Protecting against AI-enabled attacks and ransomware **are key priorities for organisations.** Underpinning this is a focus on solid systems' foundations. These priorities mirror those in the US/UK.

Next steps

Embedding a culture of cyber resilience

New cyber threats emerge every day, as evidenced by the widespread coverage of incidences such as the CrowdStrike software glitch that hit so many firms in July 2024. While it wasn't an attack perpetrated by criminals, too many Australian businesses were caught off guard by this situation.

As the results from RSM's research show, this lack of preparedness can be attributed to an inadequate culture of cyber security and resilience, insufficient risk assessments, deficient security measures and poorly-tested incident response plans.

"Implementing tailored security measures and regularly testing incident response and business continuity plans is crucial to minimise the impact of future cyber incidents," says Ashwin Pal, Partner, Security and Privacy, RSM Australia.

"Without rigorous testing, organisations may overestimate their level of preparedness, leading to disastrous outcomes during actual cyber incidents," Pal says.

Businesses must prioritise cyber security testing, including:

- Performing vulnerability assessments.
- Holding incident response drills.
- Conducting business continuity planning exercises.

"Testing should be conducted regularly and involve all relevant stakeholders to ensure the effectiveness of the business's cyber resilience measures," says Pal.

Strategic recommendations

1 Deeply embed cyber risk management processes

APRA's CPS 230 Operational Risk Management cross-industry prudential standard, effective from July 2025, emphasises the importance of managing operational risks and maintaining critical operations during disruptions as a result of cyber security incidences. While it applies specifically to financial services firms (including service providers) that report to APRA, the standard is instructive for all Australian businesses in terms of the steps they need to take to appropriately manage their cyber risks. In line with the standard's requirements, Australian businesses should:

- Identify, assess and manage cyber risks through effective internal controls and monitoring.
- Maintain a credible business continuity plan to ensure critical operations can continue during severe disruptions.
- Effectively manage risks associated with service providers through comprehensive policies, formal agreements and robust monitoring.

2 Engage in continual cyber security testing

Cyber security testing must be prioritised and integrated into core business operations. This includes:

- Incident response testing.
- Business continuity planning.
- Cloud testing.
- Exercises and scenarios.

Organisations should develop and test multiple cyber risk scenarios, increasing in intensity, to prepare for worst-case scenarios.

3 Conduct ongoing due diligence into third-party risks

Third-party risks are more significant than ever due to interconnected business networks. Entities should:

- Conduct thorough due diligence on suppliers.
- Ensure supply chain partners meet certain network security standards.
- Verify suppliers comply with standards such as the Essential 8 during contract negotiations.

Reducing this risk involves developing a deep understanding of the supply chain and asking pointed questions of suppliers.

Essential 8 refers to a set of strategies for mitigating cyber security risks. The Australian Cyber Security Centre (ACSC) developed the Essential 8 as part of its Strategies to Mitigate Cyber Security Incidents. These strategies are designed to protect systems from a range of cyber threats, including malware, ransomware, and other malicious activities.

Ultimately, cyber resilience is not just about technical controls; it requires a strategic approach that involves the entire business. By being mindful of industry standards, conducting regular risk assessments and testing and fostering a culture of resilience, Australian businesses can enhance their cyber defences and protect their operations.

About the research

This report is based on data gathered through online surveys and interviews with 150 C-suite executives and business leaders across Australia in July 2024. Insights from clients and interviews with industry experts have been incorporated to provide a comprehensive understanding of emerging threats and best practices.

Research Methodology

Online survey panel recruited

Six minute length of interview

N=150

- C-Suite Executives (CEO, CIO, CTO, COO, CSO, etc)
- Network/systems analysts, security leads, IT Managers
- Business owners

Australia nationally representative

Fieldwork: July 2024

Our Sample

- C-Suite Executives (CEO, CIO,CTO, COO, CSO, etc)
- Network/systems analysts, security leads, IT Managers
- Primary or joint decision makers for purchasing IT equipment and IT services

Gender

Males	59%
Females	41%

Company Type

Multinational commercial (publicly listed or privately owned)	24%
National commercial (publicly listed or privately owned)	34%
State based commercial (publicly listed or privately owned	19%
Government — Fed, State or Local	3%

State

NSW	31%
VIC	27%
QLD	18%
SA	7%
WA	9%
NT	1%
TAS	3%
ACT	3%

Seniority

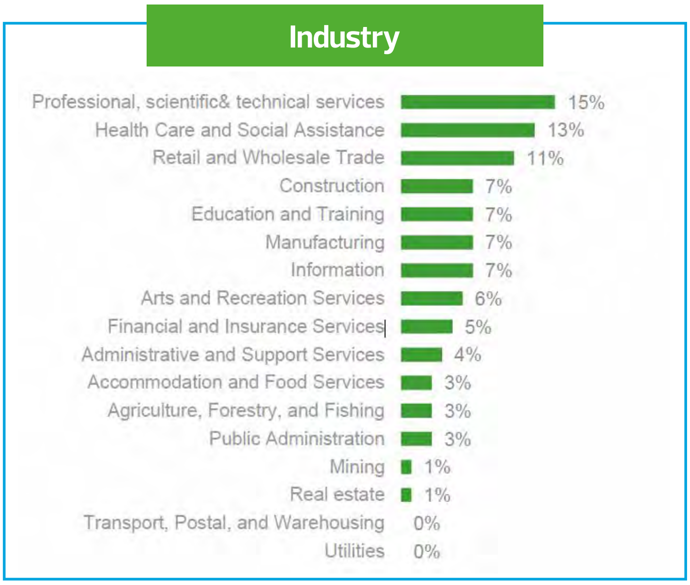
Mid-Level	15%
Senior-Level/Manager	18%
Director	19%
Executive (C-suite, Partner, Owner)	47%

Decision making

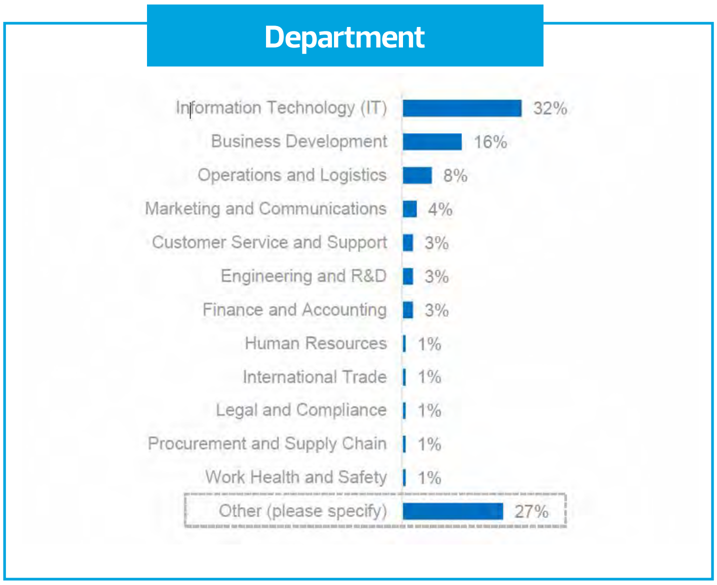
Primary decision-maker	69%
Part of a team that makes the decision together	23%

Employees

1-50 Employees	56%
51-500 Employees	21%
501+ Employees	23%



Industry



Department

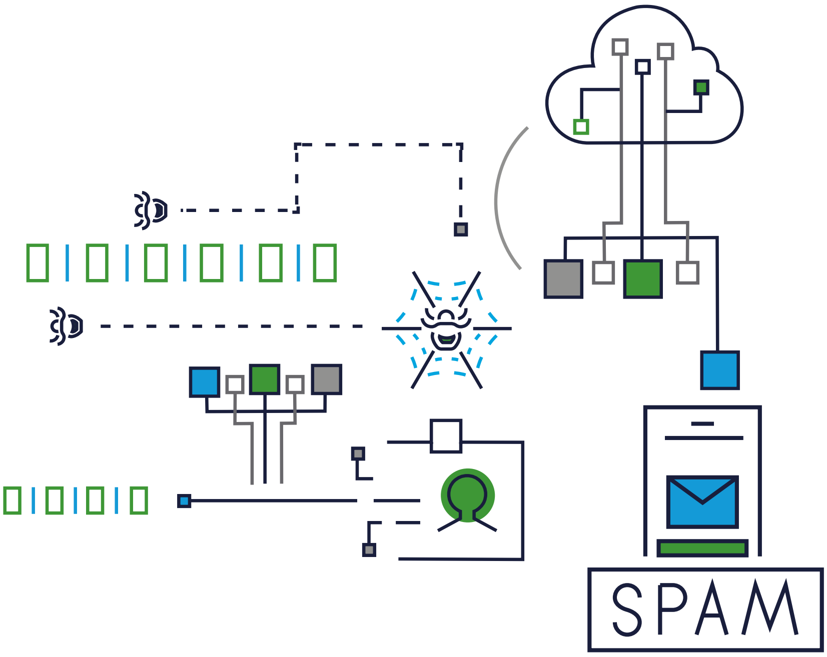
For more information get in touch with:

RSM's cyber security team

Darren Booth
Partner, Security & Privacy
T 03 9286 8158
E Darren.Booth@rsm.com.au

Ashwin Pal
Partner, Security & Privacy
T 02 8226 4858
E Ashwin.Pal@rsm.com.au

Riaan Bronkhorst
Partner, Security & Privacy
T 08 9261 9272
E Riaan.Bronkhorst@rsm.com.au



THE POWER OF BEING UNDERSTOOD
ASSURANCE | TAX | CONSULTING

rsm.com.au

RSM Australia Pty Ltd is a member of the RSM network and trades as RSM. RSM is the trading name used by the members of the RSM network.

Each member of the RSM network is an independent accounting and consulting firm, each of which practices in its own right. The RSM network is not itself a separate legal entity of any description in any jurisdiction. The network is administered by RSM International Limited, a company registered in England and Wales (company number 4040598) whose registered office is at 50 Cannon Street, London EC4N 6JJ. The brand and trademark RSM and other intellectual property rights used by members of the network are owned by RSM International Association, an association governed by article 60 et seq of the Civil Code of Switzerland whose seat is in Zug.

Liability limited by a scheme approved under professional standards legislation