



DICKER
DATA

Understanding the Cybersecurity Opportunity

with Australian Small & Medium Businesses


CISCO
Distributor


TRA
TECH RESEARCH ASIA



Table of Contents



| | |
|---|----|
| Introduction | 3 |
| Factors Shaping SMB Cybersecurity | 4 |
| Cybersecurity solutions deployed by SMBs..... | 7 |
| Cybersecurity SMB Spending | 8 |
| Marketplace Challenges and the Partner Opportunity | 9 |
| Budget Priorities for the Coming 12 Months | 10 |
| Pick me, pick me!..... | 14 |
| In closing & Partner CTA | 17 |
| Dicker Data's Key Takeaways and Next Steps for Partners | 18 |
| The Cisco Perspective | 20 |
| We are here to help | 22 |
| About | 23 |
| Demographics: Australia..... | 24 |



Introduction



Australian small and medium businesses (SMBs) face a complex, fast-moving threat landscape.

Breach disclosure laws, director liability, non-stop threat activity, growth in data estates that require protection, and the rapid development of AI augmented cybersecurity solutions (and attacks) mean cybersecurity is a critical issue for Australian SMBs.

Separate TRA research undertaken for Dicker Data into **AI adoption in Australia** found that 56% of SMBs already have AI projects in play and of these, only 37% have guidelines in place around data usage and access. With 4-in-10 Australian SMBs adopting AI solutions in an ad-hoc manner similar to a consumerisation of IT approach, SMBs are at real risk from both poorly secured AI and growth in data driven by AI content creation.

To understand the situation in Australia, Tech Research Asia (TRA) undertook a survey, on behalf of Dicker Data, with 400 Australian small and medium (SMB) businesses to understand their cybersecurity capabilities, the types of solutions businesses use, and their future plans for cybersecurity investment.

This report summarises the key research findings and provides guidance to partners on how they can capitalise on the opportunity.

Note: The data cited in this report is from a commissioned survey undertaken by TRA in April 2024. Details of the methodology and sample are provided at the end of the report.

Factors Shaping SMB Cybersecurity

The cybersecurity environment isn't getting any easier for SMBs, many of which are ill-equipped to deal with challenges in-house

There are numerous considerations for SMBs, including:

- **Frequency and persistence of threat actors:** Data from the 2023 Australian Signals Directorate (ASD) Cyber Threat Report reveals the ASD responded to 1,100 cybersecurity incidents on Australian businesses. Law enforcement agencies received notification of attacks on businesses at the rate of one report every six minutes¹, equalling approximately 87,600 reports per year.
- **Threat Vectors can be addressed by improving cybersecurity hygiene:** Compromised credentials, malicious in-house activities, and unpatched vulnerabilities persist year after year, and remain among the most common addressable weaknesses. The 2024 data shows these are still significant issues for SMBs.
- **Workplace culture:** Establishing and maintaining a strong, effective company-wide cybersecurity culture is extremely difficult, and cyber burnout and fatigue undermines performance and investments. TRA research reveals that almost 9-in-10 Australian companies experience some form of cyber fatigue or burnout amongst cybersecurity employees, and 1-in-4 firms have had employees resign as a result.

Skills shortages:

In-house SMB cybersecurity employees are in short supply, and Australian companies are estimated to be facing a shortfall of 30,000 unfilled cybersecurity positions by 2026². This shortage isn't helped by issues impacting workplace culture.




¹ <https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023>

² <https://ia.acs.org.au/article/2022/cyber-skills-gap-is-worse-than-we-thought.html>



Factors Shaping SMB Cybersecurity

- **Cybersecurity costs have increased as a proportion of IT budgets.**
From TRA's annual IT spending analysis, as a percentage of total SMB IT budgets, spending on cybersecurity has increased from 6% in June 2020 to 9% in June 2023 (fuelled by both higher salaries and increased investment in solutions)³.
- **Cybersecurity incident costs are also increasing.**
The average cost (breach, remediation and tools) of a cybercrime incident has also increased 14% from last year, with ASD data showing it now stands at \$46,000 for small businesses and \$97,200 for medium businesses.
- **Regulatory requirements and director liabilities are increasing the need to have a robust cybersecurity capability.**
The Notifiable Data Breaches (NDB) scheme and the Privacy Act require businesses to maintain a strong cybersecurity posture and report data breaches promptly. Director and board liabilities are also fuelling greater focus from senior executives on cybersecurity exposure.
- **Critical Infrastructure and AusGov Cyber Strategy.**
The 2023-2030 Australian Federal Government Cybersecurity Strategy⁴ lays out a number of key areas - such as new cyber obligations, streamlined reporting processes, improved incident response, and intelligence sharing after cyber incidents—that impact SMBs. This strategy works alongside the 2018 Security of Critical Infrastructure (SOCI)⁵ Act that stipulates cybersecurity requirements for businesses in 11 designated critical infrastructure industries.



Cybersecurity
incident costs
have increased

14%

from last year

¹ TRA Australian IT Spending, June 2020-2023

² <https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf>, accessed May 2024

³ <https://www.cisc.gov.au/legislation-regulation-and-compliance-subsite/Pages/security-of-critical-infrastructure-act-2018.aspx>, accessed May 2024

Partner Opportunity

In complexity lies opportunity and for partners there are a number of areas where they can support SMBs including:

- **Supplementing SMBs cybersecurity skills** to alleviate their in-house shortages and insulating against rapidly rising cybersecurity wage costs
- **Addressing hygiene factors** around patching, credential management can use employee access and security management
- **Addressing infrastructure and end-point complexity** through consolidation of cybersecurity, recovery and forensic tool sets
- **Reducing 'swivel chair fatigue'** of employees responding to constant security alerts to mitigate against fatigue and burnout
- **Improving risk postures** and reducing potential director and board liabilities by assisting with risk and compliance assessment and management



Changing Cost Profiles

Changing cost profiles through managed services rather than increasing direct in-house IT spending.



Cybersecurity solutions deployed by SMBs

Data on the deployment of cybersecurity solutions amongst SMBs shows there are good opportunities for partners.

Even the most commonly deployed solutions are found in just over 60% of companies, and in some areas, such as core technologies like identity and access management (IAM) and endpoint/mobile security, deployment levels are significantly lower.

Clearly, the chart below (Percentage of SMBs using cybersecurity solutions) shows varying degrees of solution deployment and the largest headroom for partner growth is in endpoint and mobile security (36% currently using), identity and access management (43% using) and security monitoring and operations (47% using).

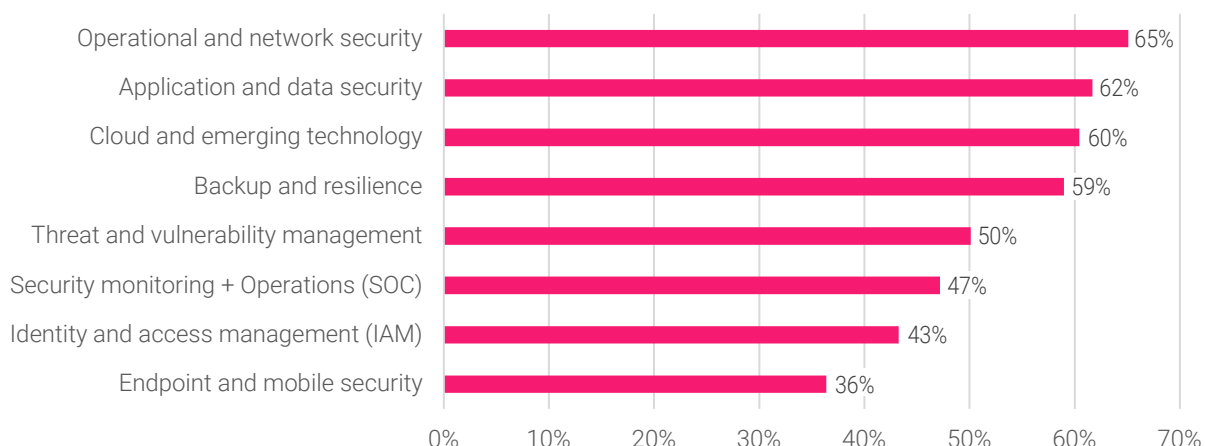


Top 3 most Deployed Solutions

- 1 Operational & network security, such as real time filtering and next generation firewalls (65% of SMBs).
- 2 Application & data security, such as application delivery controllers (ADCs), vulnerability management and attack surface management (62% of SMBs).
- 3 Cloud & emerging technologies, such as SaaS vulnerability management, IoT security (60% of SMBs).

What cybersecurity solutions are you using in your company?

■ Percentage of SMBs using cybersecurity solutions



Cybersecurity SMB Spending

1-in-2 SMBs will increase their cybersecurity spending in the coming 12 months

Reflecting the ongoing importance of cybersecurity, 46% of companies intend to increase their investment in the next 12 months, and another 46% will maintain current spending levels. 8% of SMBs have stated an intention to decrease their spending.

Of those increasing budgets, the majority (78%) are indicating relatively modest

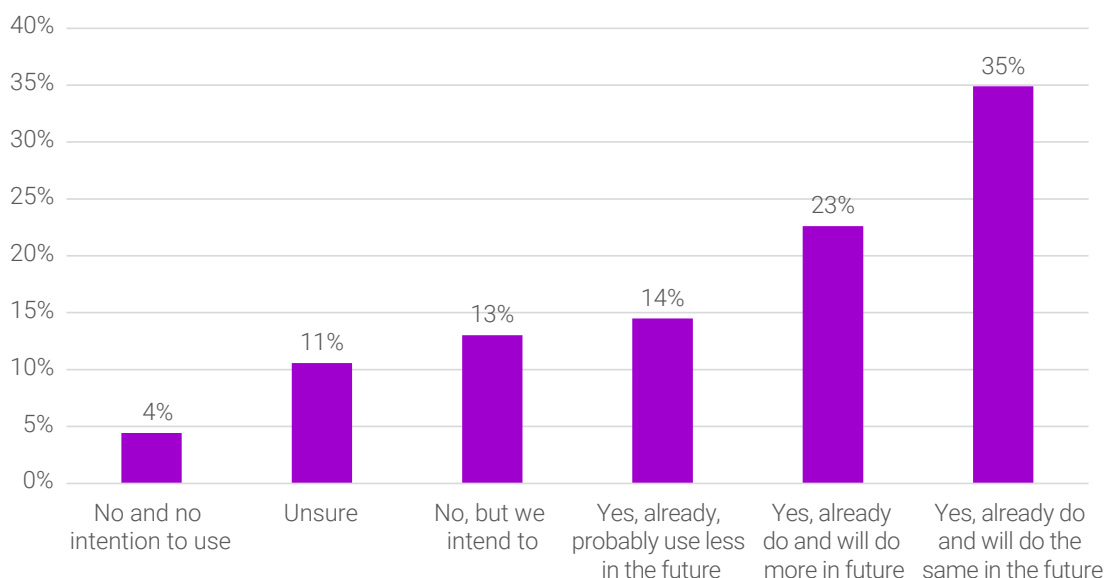
increases of between 1-10%, with 22% indicating increases greater than 10%.

59% of SMBs fund cybersecurity from within their overall IT budgets and another 27% of companies have a dedicated budget line item for cybersecurity, distinct from IT budgets. 7% allocate budget across all departments.

How those funds are spent presents a potential challenge for partners, namely, marketplaces. 72% of SMBs currently purchase cybersecurity solutions from cloud provider marketplaces (although 14% plan to reduce this activity in future) and another 13% intend to start using in the coming 12 months. (See figure 2). Only 4% of SMBs stated they have no intention to use marketplaces.

Do you buy, or do you intend to buy, cybersecurity products and services through cloud provider marketplaces?

Marketplace buying behaviour





Marketplace Challenges and the Partner Opportunity



Marketplace margins are slim, sometimes non-existent, and protecting customer incumbency can be a challenge.

Strong partners will continue to demonstrate relevancy in this channel, e.g., via services and management wraps.

Buying through marketplaces can mean SMBs are adopting a 'do it yourself' (DIY) approach. While initially appealing, this can actually leave SMBs exposed to greater complexity, integration issues,

and ultimately a weakened cybersecurity posture. Proper due diligence on solution capabilities, performance and risk is critical and there can be question marks over who holds responsibility in the result of a breach if an SMB has deployed part of a solution and a partner the other. Bringing a partner-managed service to customers can reduce this potential confusion.



DIY approach to Security can lead to complexity, integration issues and weakened security posture.

Budget Priorities for the Coming 12 Months

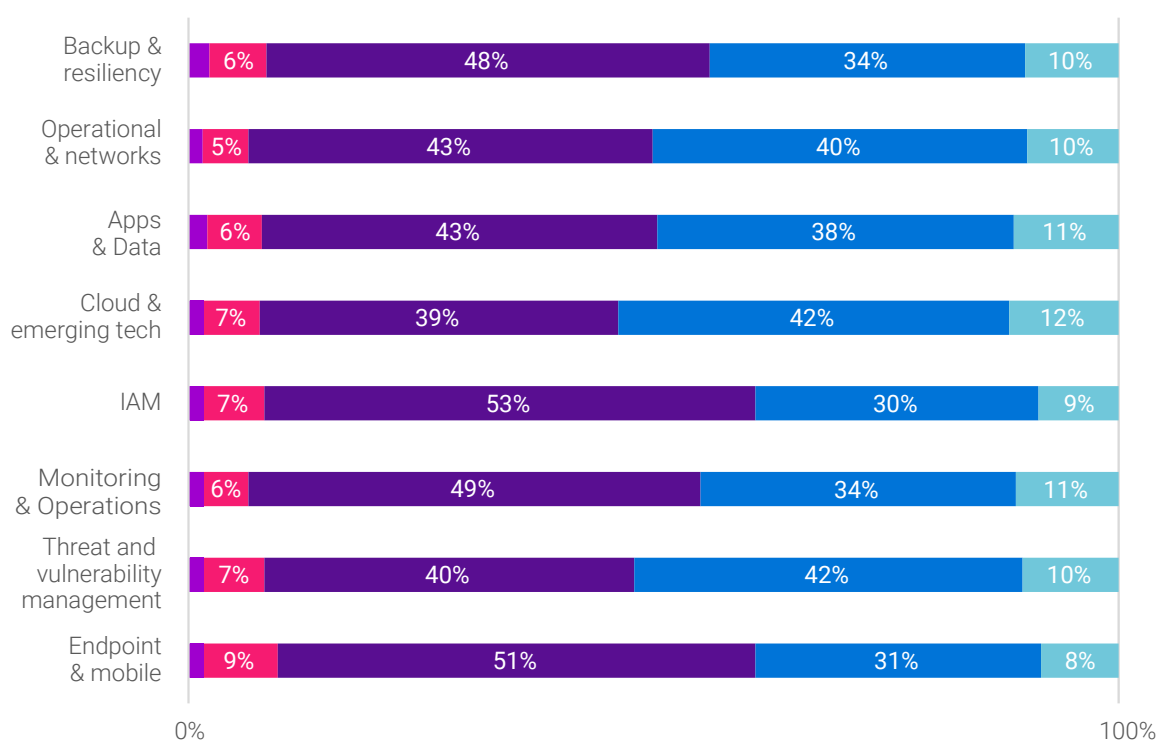
What's in the SMB cybersecurity investment plan for the next 12 months?

The data shows increases across most areas (see Figure 3), with the highest rises allocated to:

1. Cloud and emerging technologies (54% of SMBs will increase spending),
2. Threat and vulnerability management (52% of SMBs will increase spending), and
3. Applications & data and Operational & networks (50% of SMBs will increase spending in both areas).

How will your investment in cybersecurity change in the next 12 months in the following areas?

■ Decrease 10+% ■ Decrease 1-10% ■ Stay the same ■ Increase 1-10% ■ Increase 10+%

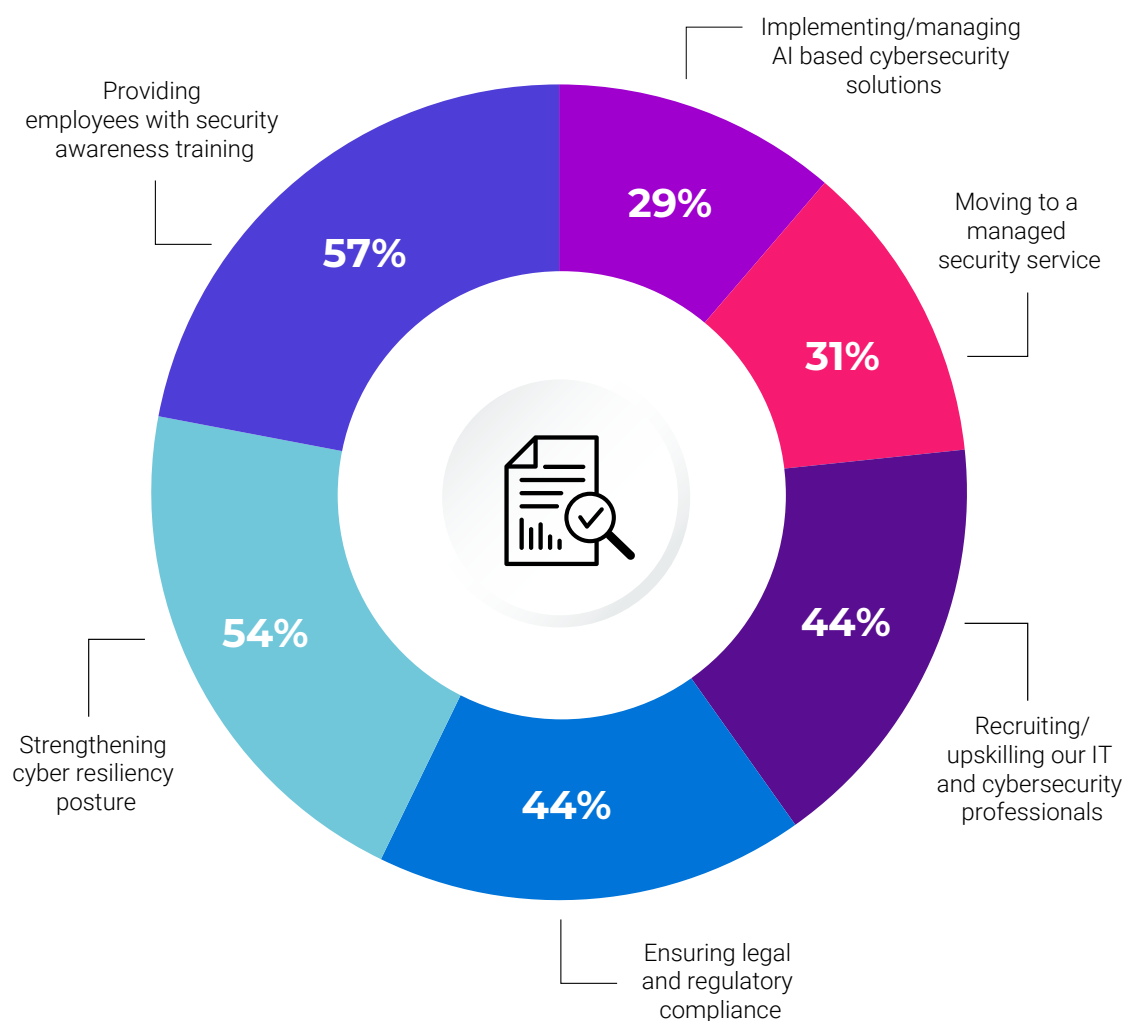


Budget Priorities for the Coming 12 Months

Outside of hardware and software spend, there are a number of services opportunities for partners including (see figure 4):

1. Providing employees with security awareness and training (57% of SMBs will invest in next 12 months),
2. Strengthening cyber resiliency posture (54% of SMBs will invest in next 12 months), and
3. Ensuring legal and regulatory compliance, and recruiting more/upskilling (in-house cybersecurity skills) (44% of SMBs in both instances).

Which of the following services will you invest in over the coming 12 months?



SMBs Need Partners

SMB Demand for outsourced services and support from partners is strong

88% of SMBs use partners to support their cybersecurity needs and operations (35% outsourcing everything to partners and another 53% having a blended partner+in-house approach). 63% of those SMBs using partners rate them at least an 8 out of 10 for satisfaction.

Identity & access management is the least outsourced (43% of SMBs keep in-house).

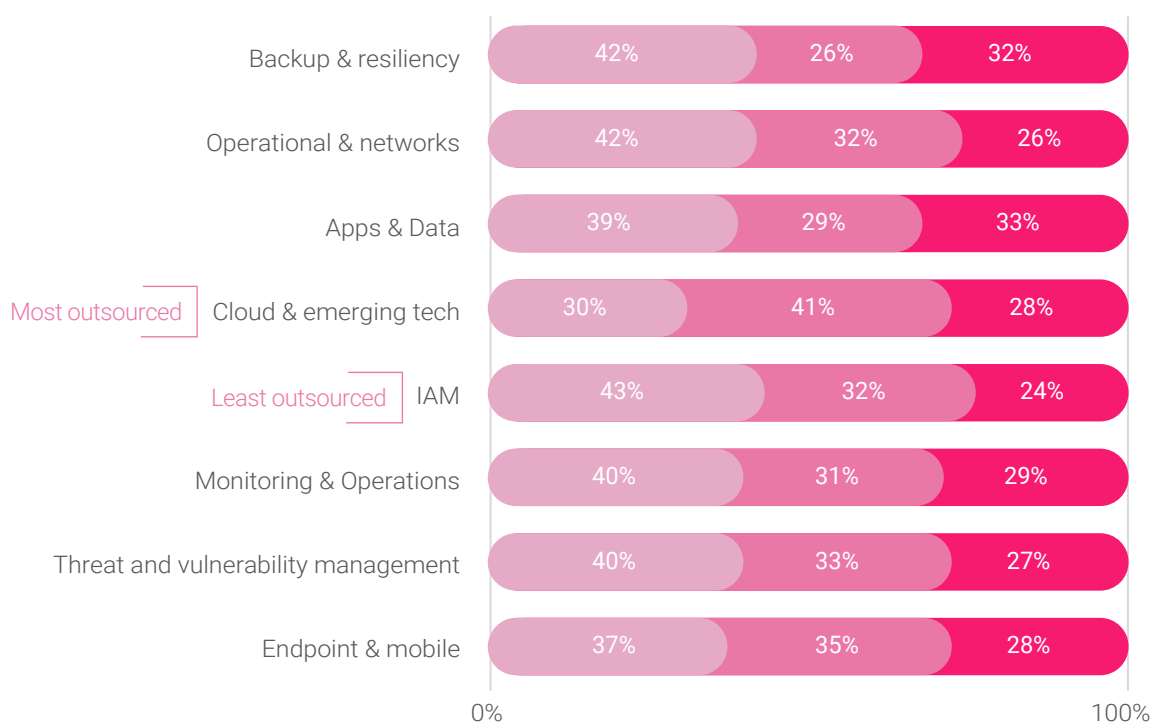


Top 3 outsourced opportunities

1. Cloud & emerging technology (70% of SMBs)
2. Endpoint & mobile (63% of SMBs)
3. Threat & vulnerability management (60% of SMBs)

Which of the following does your company currently run and manage in-house and which are outsourced?

■ In-house ■ Outsourced ■ Mix of both



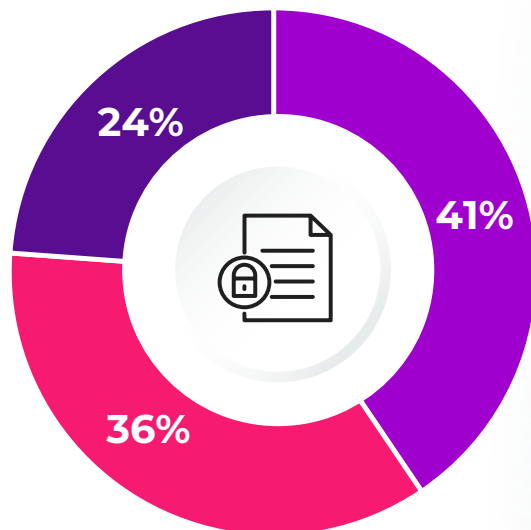
SMB Buying Behaviour

Which comes first – product, partner or vendor?

On average, the preferred SMB 'starting point' for cybersecurity buying decisions is to assess the technology products and solutions first, followed by partner selection. 41% of SMBs stated this is their initial approach (see figure 6).

36% of SMBs prefer to follow vendor recommendations on products and solutions, then look to partners for fulfilment, and 24% start with partners and follow their recommendations on products and solutions.

In your company, where do you start when buying cybersecurity solutions?



- Products & solutions 1st, then choosing a partner to deploy and/or manage
- Vendor 1st, follow their recommendation on products, solutions and partners
- Partner 1st, follow their recommendation on what products and solutions to implement

Pick me, pick me!

SMBs want cybersecurity vendors and partners to provide tailored, effective solutions that prioritise communication, affordability, and proactive threat detection. The data highlighted five key areas where SMBs look to partners and vendors for help:



Pick me, pick me!

So, what makes an SMB pick a specific partner?

Excluding price, our research shows the most important issues partners must reflect when engaging with SMBs include:

Cyber resiliency capabilities



Many SMBs now consider a breach or cybersecurity incident as inevitable, and the emphasis is now on ensuring business operations can continue even when breached. The ability to support remediation as well as business recovery with minimal disruption is a critical consideration.

Ease of integration with current in-house platforms and systems



The majority of SMBs want a single vendor platform approach rather than having to integrate multiple vendor point solutions. 63% of SMBs prefer an integrated end-to-end cybersecurity platform from a single vendor (as opposed to a multi-vendor blend of point solutions).

Brand reputation



'Reputation' blends a number of ingredients SMBs consider important, including if a vendor has a long-standing history of providing robust technology solutions, the perceived level of cybersecurity innovation in products and solutions, and customer service and support levels.

Support and use of artificial intelligence in cybersecurity solutions



AI augmented cybersecurity solutions are seen as critical to help SMBs strengthen their cybersecurity posture and capabilities. TRA data shows that SMBs are looking more to defensive AI solutions including anomaly detection, threat analysis, intrusion detection, firewall management and incident response.

SMB-focused solutions, not large enterprise



Large enterprise solutions that require complex, deep integration, extensive training and certifications, and multiple management tools simply do not work for the vast majority of SMBs. SMBs want solutions that are easy to buy, easy to understand, clear value propositions, simplified licensing agreements, backed by strong partner service and support.



Partner Opportunity



Be unique. Don't simply rehash vendor sales pitches. Instead, build your value and USPs, SMBs need your guidance and expertise.

Tailored solutions offer stronger margin opportunities and are a clear value-add for partners, especially given the higher complexity and greater need for skilled resources that accompany them.

SMBs want integrated, single-vendor environments however, this can be at odds with sourcing via marketplaces (where SMBs typically end up with multiple point product solutions to integrate and operate).

There is a potential gap here that partners can address to support SMBs.

AI-augmented cybersecurity solutions are in demand and represent a strong area of opportunity for partners. TRA research suggests there is also an additional opportunity around ensuring network, data and applications environments are 'AI-ready' alongside AI-cyber solutions.



SMBs want integrated, single-vendor environments.

In closing & Partner CTA

Overall, organisations are seeking cybersecurity vendors who can offer tailored, proactive, and cost-effective solutions while providing clear communication, education, and support throughout the implementation process.

SMBs know the cybersecurity environment is a very complex one. High profile breaches, supply chain vulnerabilities and increased regulations have accelerated SMB interest in strengthening their capabilities. The 'it won't happen to me' attitude has been replaced by an expectation of inevitable breach and subsequent recovery chaos. It is not surprising that 1-in-2 SMBs have indicated an increased spend on cybersecurity in the coming 12 months.

Partners bring clear advantages for SMBs across technology, skills, costs and education. As always though, complacency is the enemy of partner success and SMBs are looking to marketplaces as an alternative purchasing option.

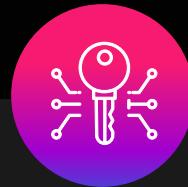
Address concerns – risk exposure, regulatory requirements, technology confusion, platform or point product integrations, costs, and AI-washing of cyber solutions – and provide tailored solutions that prioritise communication, affordability, proactive threat detection, and resiliency capabilities.



Dicker Data's Key Takeaways and Next Steps for Partners

Complexity, cost, risk and burnout have formed the perfect cybersecurity storm, exposing gaps in the digital armour of SMBs across Australia who are scrambling to stay ahead.

Businesses know they can't go it alone, with 88% of those surveyed stating they rely on partners to support their cybersecurity needs and operations. Capturing your piece of the opportunity largely depends on the maturity of your cybersecurity practice and your strategy to augment the in-house capabilities of the businesses you service.



Turnkey

SoCaaS, outsource managed services, rely on support from vendors.



Hybrid

Hybrid SoC, hybrid managed services, joint sales calls, co-branded campaigns, level 1 support in-house and escalates advanced support to vendor.



DIY

Internal 24x7 SoC, In-house managed services, sales and marketing, and wholly owned tech support.

Dicker Data's Key Takeaways and Next Steps for Partners

Businesses are looking to their technology partners to supplement their skills, and recommend solutions that can protect them in the hyper digital / AI age we now live in. This realisation is not only increasing channel dependency but is also creating a deeper understanding and appreciation of the value a modern partner brings to the cybersecurity equation. And with that, comes the willingness of businesses to allocate a larger portion of their budget to your services. However, this increased budget also comes with heightened expectations that must be managed carefully, particularly during periods of economic contraction.

It's clear that cybersecurity will be the growth engine of the Australian IT industry in 2025, followed closely by AI. With that in mind, it's critical that every partner has a cybersecurity strategy, not only to protect

your customers from cybercrime, but also to ensure your customers are still **your** customers in twelve months' time.

Cybersecurity is an outlier in an otherwise difficult market. Budgets are increasing, awareness is growing and the number of attacks are surging. Now is the time to ensure your cybersecurity offering meets the challenges facing your customers. Start a conversation with your Dicker Data representative today on how we can support you in accessing your customers' environment, exposing their vulnerabilities and compliance gaps and then finding the right Cisco solution to enhance their security posture.

Just as your customers have realised they can't go it alone, neither can you.

Contact the Dicker Data team today and discover why experience is the difference.





The Cisco Perspective

As cybersecurity needs for SMBs grow, Dicker Data, in collaboration with Cisco, is committed to supporting our partners with tailored solutions, expert guidance, and a range of resources. We are focusing on the following key initiatives to empower our partners in the Australian market:

Deploy Targeted Cisco SMB Security Solutions

1

Our research shows SMBs need simplified, scalable solutions, with a focus on cost-effectiveness and ease of deployment. Cisco's SMB bundles are specifically designed to address these needs:

- **Cisco Secure Firewall Small Business Edition** – Provides robust threat defense with cloud-based management, ideal for SMBs seeking comprehensive protection.
- **Cisco Umbrella** – Offers DNS-layer security and secure web gateway services, ensuring safe web access for employees on and off the network.
- **Cisco Duo** – Delivers multi-factor authentication to protect access to applications, ensuring secure and trusted user access.

These bundles allow partners to address SMB needs efficiently, ensuring clients benefit from integrated, manageable security. For more details, explore [Cisco Secure Firewall](#), [Cisco Umbrella](#), and [Cisco Duo](#).

Leverage Incentives for Customer Assessments

2

The report also highlights the value of proactive assessments for SMBs, with partners seeking financial support to offer these services. Cisco offers an exclusive Customer Assessment Incentive, helping partners conduct assessments that identify client vulnerabilities and guide solution recommendations. This initiative strengthens SMB trust and provides partners with an additional revenue stream. For more information on the Customer Assessment Incentive, click here: [Cisco Customer Assessment Incentive](#).

The Cisco Perspective

Reduce Management Complexity with Cisco's AI Driven Solutions

3

The reports reveal SMBs need solutions that minimise administrative burdens while maintaining robust security. In the era of AI, Cisco is committed to leading the way in connecting and protecting your infrastructure.

- **Cisco's Unified AI assistant** – Cisco AI Assistant combines the latest generative AI tech across all of Cisco's platforms bringing our expertise to responsibly guide and inform the decisions you make every day.
- **Cisco AI-Ready Infrastructure** – Provides advanced, scalable AI capabilities to simplify security administration and improve threat detection.
- **Cisco AI Readiness Index** – Assesses an SMB's readiness to implement AI solutions effectively, guiding partners in offering the right technology for each client's needs.

By integrating AI-driven solutions, partners can streamline SMB cybersecurity management, helping clients focus on business growth. Learn more about Cisco's AI capabilities here: [Cisco AI-Ready Infrastructure](#) and [Cisco AI Readiness Index](#).

Upskill Your Team with Cisco Blackbelt and Dicker Data Support

4

As partners look for cost-effective, accessible training options, Dicker Data, in collaboration with Cisco, provides a comprehensive platform for learning and certification.

Additionally, Dicker Data's dedicated Cisco Security practice supports partners with presales engineers, solutions architects, training resources, demo and proof-of-concept assistance to ensure successful solution deployment.

For further information on Dicker Data's Cisco cybersecurity offerings and resources, visit [Unlock the Cisco Cybersecurity Opportunity](#).

In conclusion

We invite our partners to collaborate with Dicker Data to deliver impactful security solutions to SMBs across Australia. Contact your Dicker Data account manager to learn how these initiatives can support your success in the SMB market and leverage Cisco's solutions, training, and incentives. Together, let's make cybersecurity accessible, effective, and tailored to meet the demands of today's SMBs.

We are here to help

Dicker Data is here to help all of our partners capitalise on the cybersecurity opportunity. Our team of experts are available to answer questions and support technology partners in deploying secure, compliant and reliable cybersecurity solutions for ANZ SMBs.

For more information contact:

sales@dickerdata.com.au

DICKER
D A T A



About

To understand the situation in Australia, Tech Research Asia (TRA) undertook a survey, on behalf of Dicker Data, with 400 Australian small and medium (SMB) businesses to understand their cybersecurity security capabilities, the types of solutions businesses use, and their future plans for cybersecurity investment. This report summarises the key research findings and provides guidance to partners on how they can capitalise on the opportunity.

TECH RESEARCH ASIA (TRA).

TRA is a fast-growing IT analyst, research, and consulting firm with an experienced and diverse team in: Australia, Singapore, Malaysia, and Tokyo. We advise executive technology buyers and suppliers across Asia Pacific. We are rigorous, fact-based, open, and transparent. And we offer research, consulting, engagement and advisory services. We also conduct our own independent research on the issues, trends, and strategies that are important to executives and other leaders that want to leverage the power of modern technology.



www.techresearch.asia

Copyright and Quotation Policy: The Tech Research Asia name and published materials are subject to trademark and copyright protection, regardless of source. Use of this research and content for an organisation's internal purposes is acceptable given appropriate attribution to Tech Research Asia. For further information on acquiring rights to use Tech Research Asia research and content please contact us via our website or directly.

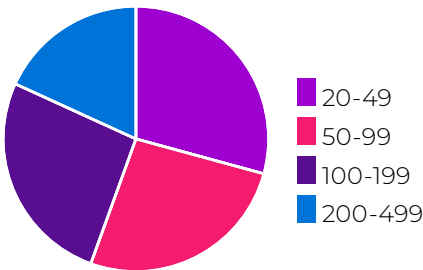
Disclaimer: You accept all risks and responsibility for losses, damages, costs and other consequences resulting directly or indirectly from using this research document and any information or material available from it. To the maximum permitted by law, Tech Research Asia excludes all liability to any person arising directly or indirectly from using this research and content and any information or material available from it. This report is provided for information purposes only. It is not a complete analysis of every material fact respecting any technology, company, industry, security or investment. Opinions expressed are subject to change without notice. Statements of fact have been obtained from sources considered reliable, but no representation is made by Tech Research Asia or any of its affiliates as to their completeness or accuracy.

Demographics: Australia

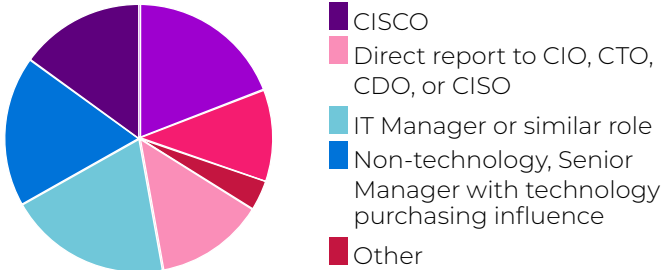


TRA undertook research via online panels across 400 Australian small and medium businesses in April 2024. Information on role of respondent, number of employees and industry sectors is shown in the charts.

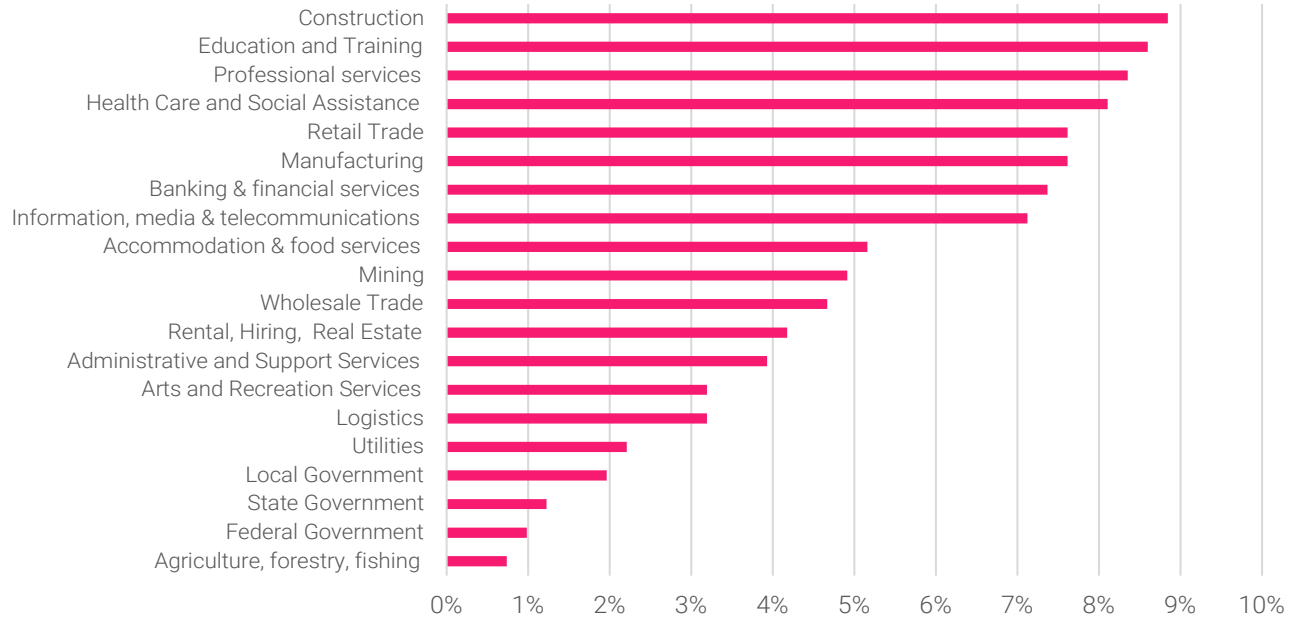
Respondent Companies by Employee Size



Respondents by Role



Demographics by Sector





DICKER
D A T A



CONTACT OUR TEAM

Australia

1800 688 586

www.dickerdata.com.au
sales@dickerdata.com.au

238 Captain Cook Drive,
Kurnell, NSW 2231

