Big cyber security questions for small business

The state of cyber fitness in Australian small businesses

Cynch Security

Deakin University

RMIT University

AustCyber Projects Fund

Contents

Authors

Cynch (Cynch Security)

The Cynch founders were colleagues at iconic Australian institution, Australia Post. They founded Cynch in 2017 after recognising how underserved small business leaders were by the cyber security industry. Cynch is dedicated to helping small business leaders prevent a cyber security incident from becoming one of the worst days of their career. They collaborate with small businesses and their trusted partners, continuously profiling their cyber risks to provide the people at the heart of these businesses with everything they need to build and demonstrate cyber fitness – in less than five minutes at a time, at a price they can afford.

Deakin University

The Deakin University Centre for Cyber Security Research and Innovation (CSRI) is a strategic research centre that works with industry and government leaders on innovative research that has real-world impact. Their researchers represent a diverse section of academic fields within Deakin and experts working within the private sector. This holistic approach to cyber security research uniquely positions them to collaborate and innovate in meaningful ways.

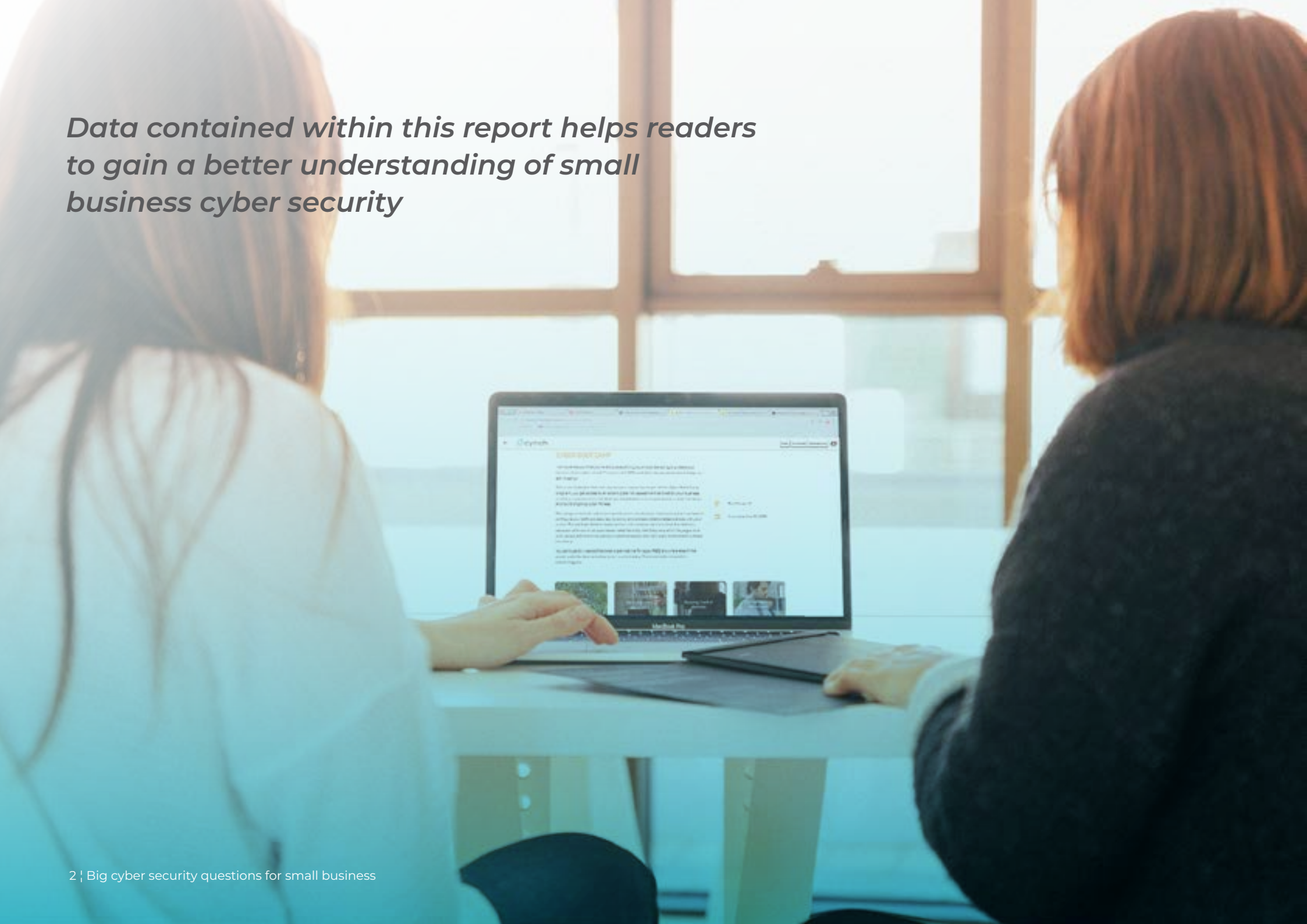
RMIT

The RMIT University Centre for Cyber Security Research and Innovation (CCSRI) was established in 2020. The focus of RMIT CCSRI is to develop a multi-disciplinary research centre relating to the organisational, human and technology aspects of Cyber Security drawing upon RMIT Cyber expertise in Australia and with expertise from RMIT Europe and RMIT Vietnam. In the innovation space the RMIT CCSRI works with the RMIT Activator and the Cloud Innovation Centre supported by Amazon Web Services.

AustCyber Projects Fund

The AustCyber Projects Fund is a $15 million, three-year initiative designed to help the Australian cyber security industry grow and take ideas global. In 2018, AustCyber provided $6.5 million in funding across ten projects that are making a real contribution to growing Australia's cyber security ecosystem. In 2019, an additional $8.5 million was awarded to fund industry led projects that deliver on the goals of the Cyber Security Sector Competitiveness Plan. This included $100,000 in funding of this project.

Data contained within this report helps readers to gain a better understanding of small business cyber security



Foreword

Over the next decade, the Australian cyber security sector will become larger, more diverse, and more sophisticated. There are now over 500 providers in the domestic sector and a closer look at Australia's 2020 Cyber Security Sector Competitiveness Plan reveals it is characterised by new, innovative small businesses which are active across the country.

This places our industry in the best possible position to support and partner with the 2.4 million small businesses in Australia to improve their cyber risk management and use cyber security as a competitive advantage.

Small businesses face pressure from all directions and keeping them secure is a complex undertaking. Attacks continue to evolve and threaten businesses that depend on technology, yet advice from experts is often inconsistent and generalised, creating confusion and, at times, apathy.

We are proud to have supported Cynch Security, Deakin University and RMIT University through AustCyber's Projects Fund to undertake a series of activities to address the growing need to understand and help small businesses address cyber risk.

Small businesses contribute around a third of Australia's GDP and employ more than 40 per cent of Australians – a lack of meaningful data means that little is known about the cyber security realities they are dealing with.

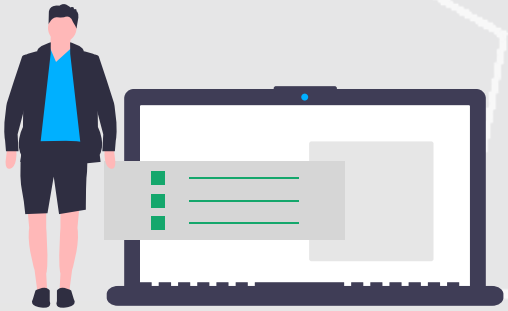
This is critical not just for these businesses as entities themselves, but also in their partnerships with each other, being involved in the supply and value chains of larger businesses and governments, and to inform ways to better support response efforts in the likely event that a cyber attack occurs.

Gathering data on attitudes and challenges, which in turn will inform and hopefully change business culture to incorporate risk, is particularly important as the impact of COVID-19 appears to have hit micro and small providers hardest as customers adapt to digitally dominant modes of working.

Despite the short to medium term disruption to some service delivery, the pandemic is likely to accelerate the long-term transformation of the economy through technology and increased demand for cyber security.

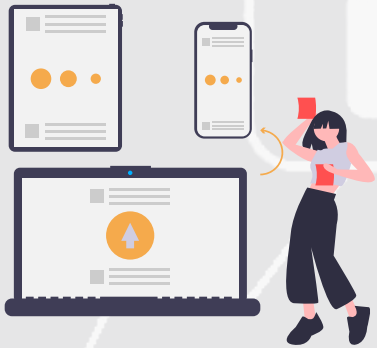
Supporting small businesses to do this safely and securely is crucial and I hope the data contained within this report helps readers to gain a better understanding of small business cyber security norms and behaviours – not just in Australia, but also globally.

Michelle Price
CEO AustCyber



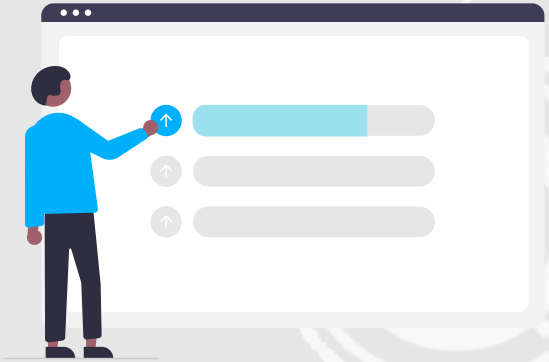
84% of Australian small businesses have **adopted online services** and rely on up to 30 separate technologies

Less than 15% of small businesses **have paid** for **outside cyber security** help in the past 12 months

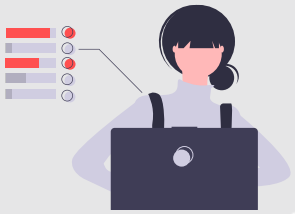


Australians report **cyber security incidents** to **cyber.gov.au** **every 10 minutes**

19% of small businesses **spent $0** on cyber security over the past 12 months



72% of small businesses consider **cyber security** as **very important** while only 50% rate physical security the same



2 out of 5 small businesses have direct experience with a **cyber incident worthy of reporting** at some level

Executive Summary

- As Australian small businesses' reliance on technology grows, so too does the potential fallout from a cyber incident. The smaller the business, the more likely that IT administration will be managed by the owner.
- Small business owners know that computer systems are inherently vulnerable, and will accept ownership of any related risks. Yet they have difficulty finding the time, available budget, appropriate support staff, and/or the knowledge about what could be done to manage cyber risk.
- Reports to Scamwatch were up almost 25% in 2020. Cyber criminals looking for ways to exploit the new digital economy have found them.
- One of the big challenges for cyber security experts is to provide information that is easily understood by the average person. They tend to speak and write in cyber security lingo — using technical terms that are baffling to most people.
- Small businesses do what they can with what they have – but recognise more needs to be done. And they would do more with a cyber security service provider by their side, but the 'business' in small business aligns them to enterprise-level solutions at a sophistication they don't need that come with a price tag they definitely can't afford. So instead they now believe expertise to be out of reach.
- While small businesses are keen to increase their investment in cyber security, the operating health of the business during this challenging period of sustained economic turmoil will likely mean the additional budget will not materialise.
- The main motivator for a business owner to consider their cyber risk is direct experience with a cyber incident – but by the time one happens, it's too late. The next best thing would be a second hand story from a close friend or trusted contact, but victims of cyber crime seem to not want to talk about it.
- The free resources on sites like cyber.gov.au look like they'd be great – but small business owners struggle to apply the lessons to their specific circumstances and set up.

[1] 'Scam statistics,' Scamwatch, retrieved 24 January 2021 from https://www.scamwatch.gov.au/scam-statistics

The definitions to know and the variables to consider when reading this white paper.

Section 1: Analysing cyber analysis

Introduction

Cynch Security, Deakin University and RMIT University, supported by AustCyber formed a colation to collaboratively embark on one of Australia's largest cyber security projects of Australian small businesses.

Little is understood about the security challenges that Australian small business owners face. Which is shocking, when you consider their number. Australian businesses are overwhelmingly small: 97% of all Australian businesses have fewer than 20 staff[2]. That 97% speaks for two thirds of all Australian jobs.

Small businesses are fighting for survival because of the COVID-19 crisis. A survey[3] conducted one year into the global health crisis and economic downturn revealed that 60% of small and medium-sized businesses in Australia and New Zealand are operating in crisis or survival mode. The unprecedented times and rapid pace of digital adoption has left too many operating touch-and-go, exposing them to threats for which they are unprepared.

The Australian Cyber Security Center (ACSC) receives 1 cyber incident report every 10 minutes[4].

"The impacts of the lockdowns and work-at-home directives have... exposed [small and medium sized businesses] shortcomings in connectivity, support, security, and sourcing. Business resiliency of these [small and medium businesses] was put to the test as their IT systems adapted to a new operating environment."

Chris Morris,
Vice President, Cloud Services and Partner at IDC Asia Pacific[3]

[2] Small business counts: Small business in the Australian economy,' Australian Small Business and Family Enterprise Ombudsman, retrieved 24 January 2021 from https://www.asbfeo.gov.au/sites/default/files/documents/ASBFEO-small-business-counts2019.pdf

[3] 'IDC A/NZ Survey Finds 60% Of SMBs Are In Survival Mode Due To The Pandemic, But Expect To Increase IT Spending In 2021,' Scoop, retrieved 24 January 2021 from https://www.scoop.co.nz/stories/BU2101/S00080/idc-anz-survey-finds-60-of-smbs-are-in-survival-mode-due-to-the-pandemic-but-expect-to-increase-it-spending-in-2021.htm

Unfit factors:

Throughout this paper, you'll see 'Unfit factors' in boxes like this. This is where we'll share our cyber security expertise to let you know the indicators we see that are stopping small business from achieving cyber fitness.

We'll give you a quick cyber fitness workout for each unfit factor on the spot, and circle back to these factors at the end of the paper.

Limited budgets, an absence of IT staff for support, and the complexity of cyber security solutions[5] has left small businesses exposed in unfamiliar ways, with many unprepared against potentially devastating cyber incidents. There has never been a more important time to understand this sector's challenges.

To gain a better understanding of these challenges, a coalition formed between Cynch Security, Deakin University and RMIT University, supported by AustCyber. Collaboratively, they embarked on one of Australia's largest cyber security projects to research the cyber fitness of Australian small businesses.

Research methods

This project's research objective is to determine the cyber fitness of Australian small business, in terms of cyber security preparedness, risk, engagement, confidence, culture, awareness, and resilience, including potential common cyber security gaps that exist within the Australian small business community.

This paper is based primarily on **165 responses to an Australia-wide cyber fitness survey**. Supplementing and supporting the results of the survey are insights gained from t**hree micro focus groups** comprising detailed interviews with business owners, and the experiences shared by **145 cyber boot camp participants**.

[4] 'ACSC Annual Cyber Threat Report July 2019 to June 2020,' Australian Cyber Security Centre, retrieved 24 January 2021 from https://www.cyber.gov.au/sites/default/files/2020-09/ACSC-Annual-Cyber-Threat-Report-2019-20.pdf

[5] 'Cyber Security and Australian Small Business,' Australian Cyber Security Centre, retrieved 24 January 2021 from https://www.cyber.gov.au/sites/default/files/2020-11/ACSC%20Small%20Business%20Survey%20Results.pdf

Cynch Cyber Boot Camp cyber security crash course

Cynch offered a complimentary Cyber Boot Camp to survey participants and Australian small businesses between August-December 2020 to overlap with this survey. Designed to be completed over six weeks, through the program participating small businesses received:

- an automated risk assessment;
- tailored, plain-language cyber fitness support across common areas of concern;
- a report highlighting steps taken, and;
- advice on further measures they could take.

Paid support packages of six sessions with a Cynch coach were available for participants who benefit from greater assistance.

A total of 145 individuals, who voluntarily self-sorted into associations with **46 small businesses**, participated in the Cyber Boot Camp during the study.

What is cyber fitness?

Cyber fitness is a way to think about cyber risk management like physical fitness: a continual journey towards the ideal condition; a dedication to completing exercises that improve fitness gradually over time. Cyber fitness exercises work on specific factors of your business to build cyber resilience. A continual investment of resources into cyber security outcomes keeps a business cyber fit.

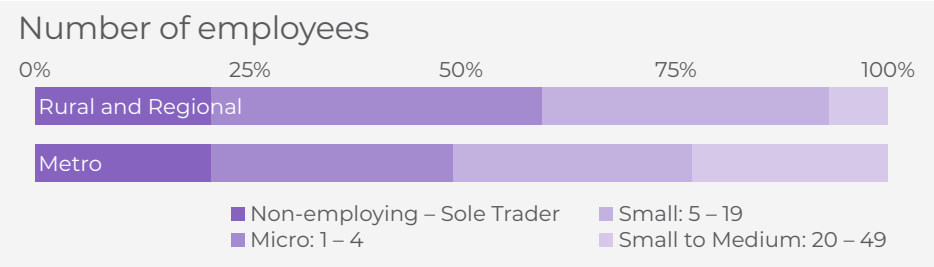
Small business data set

The Australian Bureau of Statistics (ABS) defines a small business as one that employs fewer than 20 people[6]. ABS data further separates small businesses based on the same employee count as small, micro or non-employing (self employed or sole traders). To provide a contrast to the small business sector, a limited number of small-medium sized businesses were invited to participate in the survey.

This study's business cohorts by employee count are:

Business classification	# of employees
Non-employing	Sole trader
Micro	1-4
Small	5-19
Small-medium	20-49

The employee count of each respondent's business was as follows:



78% of survey participants came from businesses with fewer than 20 employees. While a lower representative sample than the 97% of small businesses indicated in ABS data, it provides some interesting points of comparison to discuss.

[6] 'Definitions and data sources for small business in Australia: a quick guide,' Parliament of Australia, retrieved 24 January 2021 from https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/rp1516/Quick_Guides/Data

Survey responders, by the numbers

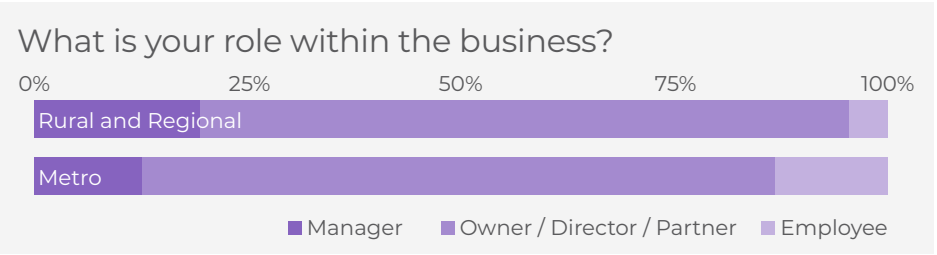
Respondents to the survey formed a broad representative sample of industries in the small business sector:

Sector	Count	%
All	51	100
Professional, Scientific and Technical Services	30	18.2
Information Media and Telecommunications	25	15.2
Education and Training	15	9.09
Other, please specify ...	15	9.09
Retail Trade	12	7.27
Construction	9	5.45
Financial and Insurance Services	9	5.45
Healthcare and Social Assistance	8	4.85
Arts and Recreation Services	7	4.24
Manufacturing	7	7.24
Agriculture, Forestry and Fishing	6	3.64
Accommodation and Food Services	4	2.42
Public Administration and Safety	4	2.42
Rental, Hiring and Real Estate Services	4	2.42

The most common organisations to respond (18.2%) were in the professional, scientific and technical services sector. The information media and telecommunications industry sectors were the next most common group of respondents, representing 15.2%.

65% of respondents are located in a metropolitan area, and **35% are located in a rural and regional area.** While businesses from six of the seven Australian states and territories responded to the survey, there is an over-representation of opinions from the larger eastern states. Around 90% of responses came from NSW, Queensland and Victoria.

The research team actively engaged with start-up communities to distribute this study: **31% of respondents identify as a start-up**.



Most respondents **(73%) identified themselves as an owner, director, partner or manager**.

Did recent measures like working from home create a cyber risk?

Section 2: Risking cyber risk

The digitisation of Australian small business

It's increasingly rare to encounter a business that hasn't digitised at least one major function. Whether they adopted a cloud accounting solution to meet single-touch payroll obligations; embraced remote working during lockdowns and beyond; or introduced new solutions to remain competitive, technology now forms an integral part of many businesses. **Small businesses that have partnered with Cynch have registered 10 technologies in use, on average**. Some businesses **use more than 30 individual technologies**.

As a business' reliance on technology grows, so too does the potential harm of a cyber incident. The fall out from a cyber attack can be much more than a mild inconvenience – improper handling of a single malicious email could lead to months of revenue disappearing overnight.

Survey respondents are aware of the role that technology occupies in their work life: across the board, be it regional or metro, Queensland or Victoria, micro or small-medium: **95% of respondents said that technology was at least somewhat important to their business**; and the majority (**88%) indicated technology is very important to their business**.

Websites, devices and applications (traditional, mobile and cloud) were all consistently identified as important to small businesses. In particular, sole traders place more importance on their business website than larger respondents.

Small businesses are embracing emerging technologies, with **social media and cloud services playing a role in 64% of businesses**. Participants are proactive in their digitisation: **84% have adopted some form of online service**.

The swift digitisation of small business has exposed a new level of vulnerability to cyber risk. Left untreated, it could lead to disaster.

Businesses don't understand their cyber risks and responsibilities

If businesses don't understand their cyber risk and work to understand the threat, they won't be able to recognise an incident or report risks that threaten to become reality.

Teams should be aware of cyber threats, and how they work. Consider bringing up cyber threats as part of a regular all staff meeting, or sending an email to your team to keep them informed. That way they'll know an attempt when they see one

Accepting ownership

Most small business owners recognise that while risks related to non-core aspects of their operation can be outsourced, any fall out could still impact them personally. **Most respondents (87%) accept ultimate responsibility for any risks associated with their business**.

As great as that positive first step is, the prevalence of consequent steps taken to manage that risk is underwhelming. **Less than half (47%) review their incident response plan regularly**.

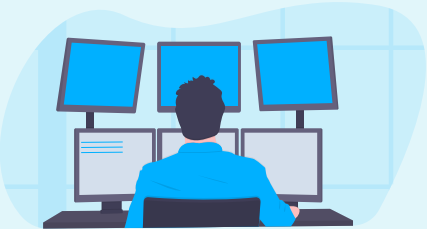
3**9% of respondents have formal cyber risk review processes in place**; and 4**7% review them on an ad-hoc basis**.

77% feel directly responsible for cyber risk, with rural and regional businesses holding more responsibility for cyber security risks than those in a metropolitan area (**76% compared to 64.6%**). **55% delegate support duties** while **61% retain security responsibilities**.

The smaller the business, the more likely day-to-day IT tasks will be managed by the owner. Compared to businesses in metropolitan areas, more rural and regional business owners handle day-to-day IT management (**48.9% of metro businesses vs 70.6% of regional businesses**). While 55% of businesses take care of IT themselves, **61% of businesses have kept IT security in-house**.

Not just a problem for 'the IT guy'

There's a common sentiment that believes cyber security concerns are something for 'the IT guys' to sort out. While IT support providers can play a critical role in managing the cyber risk of a small business, business owners should (and do) recognise the risk isn't something they can afford to outsource.



Respondents were asked how important physical security and cyber security are to their business.

Importance of cyber security	Count	%
All	133	100
Very important	96	72.18
Somewhat important	7	20.30
Neither important nor unimportant	7	5.26
Somewhat unimportant	2	1.50
Not at all important	1	0.75

Importance of physical security	Count	%
All	141	100
Very important	70	49.65
Somewhat important	48	34.04
Neither important nor unimportant	7	4.96
Somewhat unimportant	8	5.67
Not at all important	8	5.67

Businesses know that solving cyber security issues can involve something broader than just technology. Yet they remain unclear about what they need for their business to be cyber secure in the ever-changing cyber security landscape.

How do small businesses learn about cyber risk?

Where do you source information about cyber security?

29%	21%	17%	14%	12%
Business or industry communities	Technology partners%	Government websites	Personal networks	Media

The size of a business and its location does not affect how small business owners say they are staying abreast on the comings and goings of cyber security.

Preferred govt. cyber security information source

27%	18%	18%	18%
cyber.gov.au	scamwatch.gov.au	ato.gov.au	business.gov.au

There is a divide between city businesses and country businesses when it comes to staying abreast of cyber security:

	Metropolitan	Regional
ato.gov.au	13%	26%
scamwatch.gov.au	16%	24%
cyber.gov.au	36%	19%

A recent push to make cyber.gov.au the destination for cyber security related content in Australia seems well placed to simplify the process for a small business to stay informed. The Cyber Security Business Connect and Protect Program[7] will help trusted organisations raise awareness of cyber security risk and promote action in their ecosystems is likewise well positioned to amplify these existing information channels.

To gauge threat awareness levels of small businesses, participants were asked the three most common cyber security events affecting small businesses, based on those listed on report.cyber.gov.au. The most common threats suggested by respondents were:

1. A business receives an email from an unknown individual, blackmailing or demanding something (e.g. pay money or share information).
2. Malware was found on a business computer.
3. Someone in a business receives an email with new or updated bank details to deceive them into transferring money.
4. Someone pretending to be from a business emailed a customer asking them to do something (e.g. request payment or share sensitive information).

Again the size and location of a business didn't affect these responses, suggesting awareness and experience is similar across the small business sector.

How small is too small?

Cyber criminals don't discriminate on size, but the smallest of small businesses believe they are too small to be worth the effort. Less than half of sole traders see themselves as a target for cyber crime, whereas more than three quarters of small-medium businesses felt they might be valuable enough to attract unwanted attention.

Similar options are presented as part of the Cyber Boot Camp, with ransomware and email-based threats rated as participant priorities. Participants are less likely to seek help to avoid a malware infection, instead opting to improve their response capabilities and information handling practices. Proactive steps like these are key to building cyber fitness and are a promising sign that small businesses will approach this problem effectively when presented with the right solutions.

[7] Funding for business advisors to improve cyber security awareness and capabilities of SMEs,' business.gov.au, retrieved 24 January 2021 from https://business.gov.au/grants-and-programs/cyber-security-business-connect-and-protect

Small businesses interviewed as part of this study understood that cyber risk is an ongoing concern and not something that they can 'set and forget'. However, awareness of the risks is not the constraint to action. Participants would prefer increased visibility of what measures are appropriate – along with an awareness of the potential cost.

No one is sharing stories about cyber incidents

Business owners don't give cyber risk serious consideration until a cyber incident happens to them – by then, it's too late. When they realise that a cyber attack can be so crushing on a professional and personal level, they wouldn't wish it on their worst enemy.

Talk to your team, and your peers, about cyber fitness readily and openly. Sharing your story will make everyone more prepared, preventing similar incidents causing more harm...

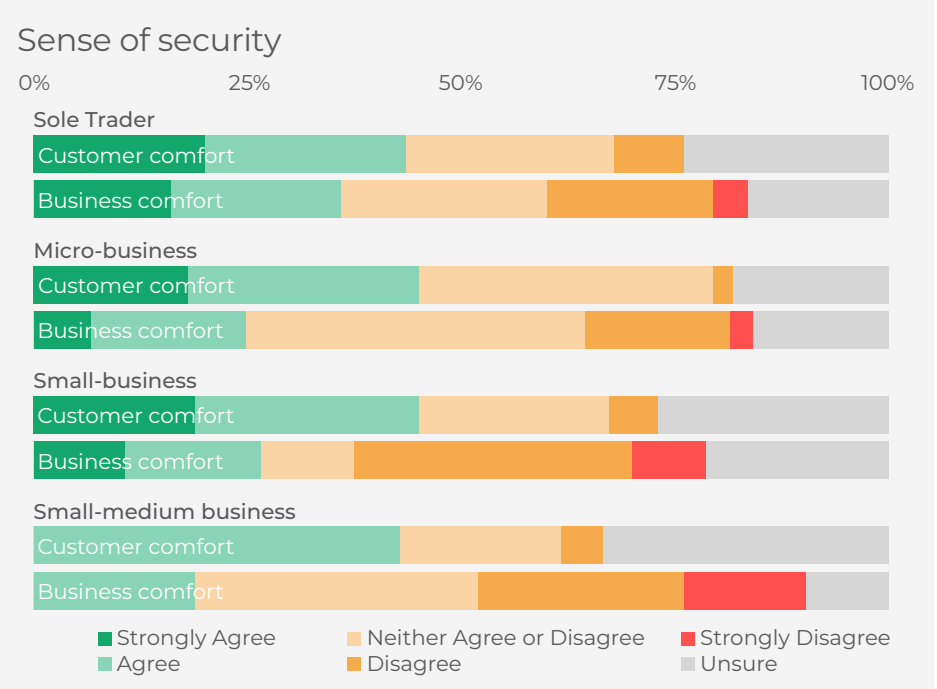
How are small businesses currently attempting cyber fitness?

Section 3: Securing cyber security

Sense of security

ACSC's 2019 small business survey[8] compared adoption of cyber security controls to understanding of cyber security concepts to see how confidence affected cyber security practices. ACSC noted "Australian [small businesses] need to better understand the risk and impact of a cyber incident" and that they "face the inherent problem of a lack of positive reinforcement for good cyber security practices". While this study did not explicitly set out to measure small business owner knowledge, we were interested in understanding business confidence and how customer perception may act as an influencing factor.

When asked if they had done enough to keep their business safe from cyber security incidents, only 26% felt that they had, while 33% felt that they hadn't. Smaller businesses were more confident, as 36% of sole traders felt they had done enough compared with 19% of small-medium businesses. When raising this topic with small businesses directly, an awareness that more needed to be done was not an issue – rather, most shared that allocating funding and time to cyber fitness was the largest contributing factor.



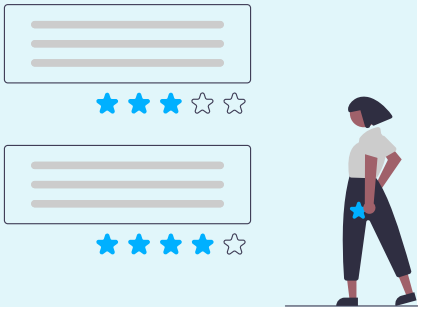
While most small businesses feel they could be doing more, half believe that their customers or clients are comfortable with the steps they've taken to protect customer information. A 64.8% majority of small-sized businesses (5-19 employees) believe that they are doing enough to protect their customer information compared to 44% of sole-traders, 45.5% of micro and 42.9% of small-to-medium. No small-medium sized business 'strongly agreed' with this statement.

[8] 'Cyber Security and Australian Small Business,' Australian Cyber Security Centre, retrieved 24 January 2021 from https://www.cyber.gov.au/sites/default/files/2020-11/ACSC%20Small%20Business%20Survey%20Results.pdf

Do small business customers care?

Tech giants like Apple have increased their use of privacy and security in marketing towards an increasingly cyber aware consumer market. At the same time industry regulation and corporate procurement programs have increased their focus towards the security of supply chains, many of which rely on services provided by small businesses.

With half of small businesses comfortable that they're meeting their customers' expectations, these trends may not have reached the sector in a significant way yet.



With many small businesses feeling that they could be doing more and that their customers or clients may not be comfortable with the steps they've taken, what are they currently doing?

How do small businesses keep cyber fit?

Cyber risk is most effectively mitigated when technical, behavioural and procedural strategies are used. Larger organisations spend millions on technical solutions alone, and still experience data breaches and cyber incidents.

To better understand how smaller businesses manage cyber risk, we asked a series of plain-language questions on a range of key control areas.

Small business and the Essential Eight

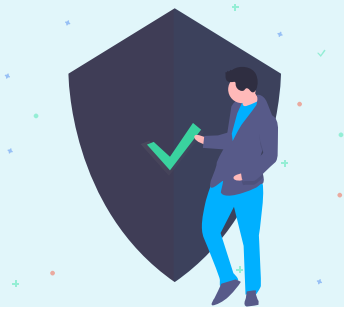
The eight security controls that make up the ACSC's Essential Eight are based on requirements from their Information Security Manual[9], but prioritised over all others due to their proven effectiveness in mitigating security incidents. For most businesses, the Essential Eight are a fantastic place to start when looking to mature the technical aspects of cyber security. Naturally, ACSC chose to base their 2019 small business survey around the Essential Eight, providing us with an interesting comparison point.

[9] 'Essential Eight to ISM Mapping,' Australian Cyber Security Centre, retrieved on 21 January 2021 from https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-ism-mapping

The plain-language Essential Eight

The ACSC 2019 small business survey asked small businesses which Essential Eight security practices they had adopted. Contrary to the study findings suggesting the use of plain-language, questions were asked using industry terminology such as 'Application hardening' and 'Patching operating systems'. The approach taken in the 2020 cyber fitness survey was to use plain-language terms to determine if a particular control had been implemented, such as "How long until a backup of an important document changed today gets stored somewhere other than your office?"

While the responses don't capture the full intent of the Essential Eight strategies, differences in the results of the two question sets speaks to the importance of avoiding technical jargon when working with a broad audience.



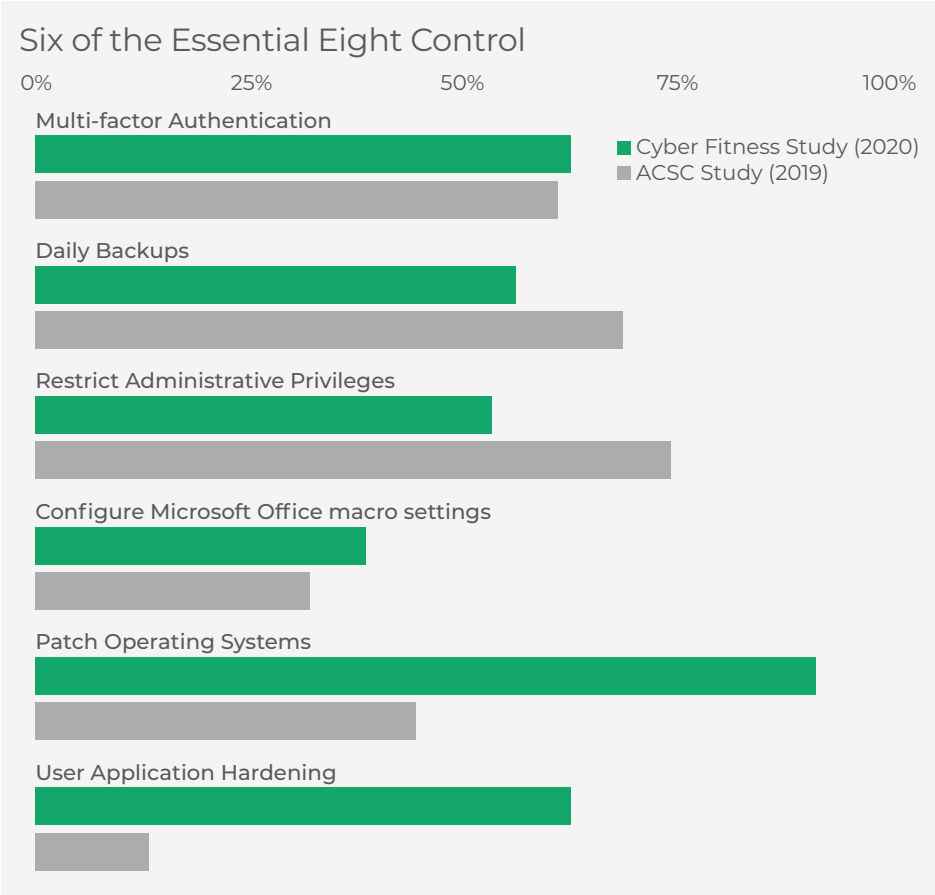
85% of survey participants agreed to share information about the cyber security measures adopted by their businesses. Six of the Essential Eight controls were assessed as part of the survey[10].

[10] For brevity, patching applications was not asked as part of the survey, in part as operating system patching provided a reasonable insight into general approaches to patching. Application control was also excluded from the study due to the technical challenges associated with implementing such controls in a small business context.

Bamboozled by tech jargon

Even great IT professionals can get too passionate about sharing the technical side of what they do in the language and specific terms as they understand them. They may not realise that what they think sounds authoritative and switched on, to the customer it's meaningless nonsense that makes them switch off and stop listening.

Cyber security professionals should endeavour to use plain language wherever possible.



Multi-factor authentication

62% of survey respondents would require some form of second factor to access their email on a new device. MFA is now a requirement of all Australian-based cloud accounting platforms, so most (if not all) small business owners would be familiar with this control – yet there appears to be reluctance to implement it on other key systems. This is even more surprising considering the concerns over email-based attacks from earlier in the survey.

Daily backup

Most respondents (56%) indicated that a backup of an important document would be stored somewhere other than their office within a day. The need for a daily backup is becoming increasingly confusing for businesses that are now operating largely in the cloud. For many small businesses, cloud sync and store solutions such as Dropbox, Microsoft OneDrive or Google Drive, have become core parts of their digital operations. Small-medium businesses in particular have embraced these solutions, or alternatively the practice of daily off-site backup, with 83% indicating same day backups were in place as compared with just 45% of sole-traders.

Restrict administrative privileges

In the ACSC 2019 small business study, restricting administrative privileges was the most common control implemented, with 74% of businesses implementing the practice.

When asked what steps would need to be taken to install software, 40% of small businesses suggested they could just run the installation package. Only half suggested they would need approval or an admin password to proceed.

While small businesses may restrict admin privileges in certain areas, such as core business software, this key concept is being followed inconsistently. The results of ACSC study show that small businesses are comfortable with the concept, suggesting the only thing needed to increase adoption is simply the knowledge that they have the ability to restrict privilege in systems.

Configure Microsoft Office macro settings

Microsoft have improved the default configuration for many of their products over recent years, including Microsoft Office, yet malicious Office macros remain a significant threat. 38% of survey respondents indicated that their Microsoft Office macros had been disabled, but 43% were uncertain.

Smaller businesses (45-51% of sole traders and micro businesses) were also more likely to have disabled macros than larger businesses (23% of small and 17% of small-medium). This may indicate that smaller teams are more familiar with the configuration of the systems used by staff.

Patch operating systems

Small businesses have embraced monthly patch cycles. An overwhelming majority of respondents (91%) indicated that an update had been installed on their computer within the last month.

Only 44% of respondents to the ACSC's 2019 study had patched operating systems. This significant gap in results may be explained by the reframing of the question.

User application hardening

62% of businesses indicated they were using an ad blocker with their web browser. This is a strikingly large number against the 12% of respondents to the 2019 ACSC study indicating the same. While an ad blocker is only one application hardening consideration, the gap in these results does suggest the term 'hardening' may not be well understood outside of cyber professional circles. Such a strong adoption rate also indicates security solutions that provide a secondary benefit (i.e. removing annoying web ads) and are simple to implement (i.e. through a browser plugin) may be more readily adopted.

Cyber incident response plan

How a cyber security incident response is managed can be the difference between a minor hiccup and a major catastrophe. The old adage rings true: if you fail to plan, you plan to fail.

Two thirds of respondents (61.5%) reported that they had not experienced, or are unaware of, any cyber security incident occurring in their business. Of those that had an incident, 1 in 20 indicated that they would prefer not to discuss it. Those that were happy to share most commonly reported their incident to the police, their IT support provider, bank and ACORN (now known as ReportCyber[11]). Just one business reported an incident to OAIC, presumably to meet their obligations under the Privacy Act.

Where are all the small business war stories?

Two out of five small businesses have direct experience with a cyber incident worthy of reporting at some level. Even with so many incidents occurring, these stories are rarely shared publicly. It's likely most would prefer to simply deal with the issue as quickly as possible and get back to business. Without an incentive to share, small business cyber incidents are likely to remain behind closed doors and obscure the fact that it really could happen to anyone.

ACSC's 2019 Cyber Security and Australian Small Businesses report stresses that "case studies should be used in cyber security advice because it will help Australian SMBs to better assess cyber risks and prioritise cyber security practices". We look forward to hearing more case studies and seeing the shift in attitude and behaviour as a result.

[11] https://www.cyber.gov.au/acsc/report

The worst time to discover you don't have access to the right people is when you desperately need help to manage a crisis. Sadly, when asked whose contact details were documented in their security incident response plan, a third of respondents had a no plan at all.

For those with a plan, the most common contacts were their IT support, a team mate, and their executive team or board. Insurers, legal counsel, police and OAIC were mentioned multiple times. Notably, larger businesses are almost twice as likely to have IT support contact information in their response plan.

The relatively small number of plans that listed the contact details for cyber insurers – just 7%, compared to the 40% who said they have some form of cover – means businesses are not taking advantage of a benefit provided by a cyber insurance policy.

It is unlikely that the Notifiable Data Breaches scheme only applies to the 4% of businesses that included OAIC's details in their response plan, which indicates most businesses are unaware of their obligations under the Privacy Act.

Government services were listed in plans infrequently, which suggests most businesses would not immediately seek the support of services such as the planned cyber emergency hotline, outlined in the 2020 cyber strategy. This service could play a critical role in helping small businesses deal with the significant harms of a cyber incident. The hotline number should be added to response plans once available.

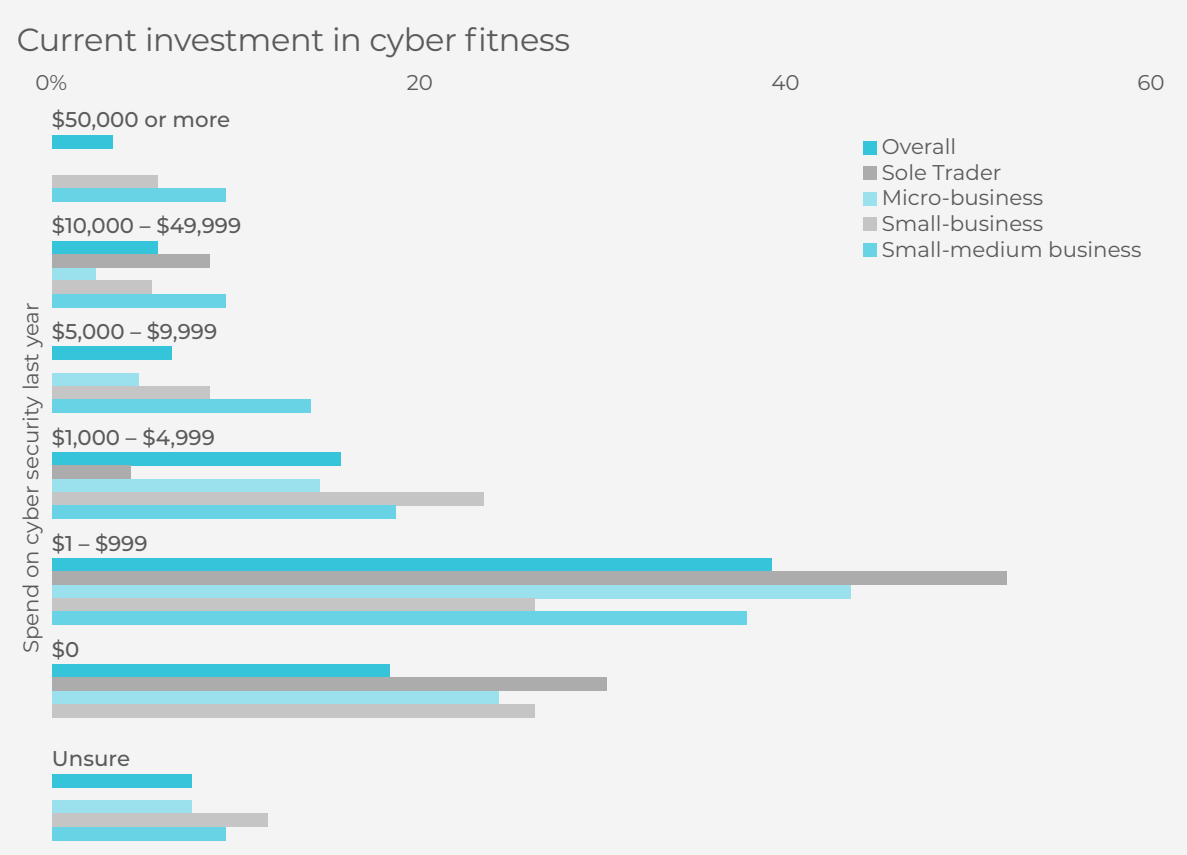
How can cyber fitness be meaningfully incorporated in a small business?

Section 4: Fitting in cyber fitness

Current investment in cyber fitness

Smaller businesses are often constrained by smaller budgets. In an industry awash with expensive solutions and consultants, even the most motivated small business will struggle to find a cyber fitness solution suitable to their needs.

Whether due to a lack of options or simply a lack of available budget, 19% of respondents invested $0 into the cyber security of their business in the previous year.



Solutions are priced out of contention

Many small business owners would do so much more if they could. But when a three-person team running a modestly successful passion project enquire about cyber security business package, providing them an enterprise level solution with a cost to match will let that business know they have no reason to consider cyber security – that it's just something for the big kids.

Start making smaller changes with the resources you already have. Every action you take towards cyber fitness, however small, provides some benefit.

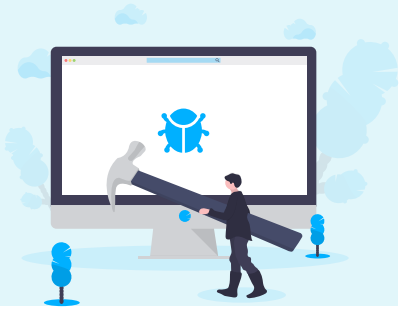
Conversely, the larger the business the larger the spend. Of those that did invest in their cyber fitness in the last year, 35% of metropolitan businesses spent $1,000 or more compared with 27% of their rural counterparts.

The CISO Lens Benchmark 2020[12] report includes insights on the approach to security investments within large Australian organisations that contrast these results. The report suggests less mature organisations often use a percentage of their IT budget when setting a security budge – 7.5% on average – while more sophisticated organisations prefer an amount per full-time equivalent employee – the average being $2,799.

If we apply the same approach to small businesses with staff, the average budget per full-time equivalent employee falls within the $100-1,000 range.

No magic bullet

Very few respondents (6%) agreed that cyber security problems could be fixed with a once-off investment. Few businesses (15.5%) felt protected because they used well-known products. These results are encouraging: it means that most understand that there isn't a magic bullet that will solve all cyber woes, and that ongoing effort is necessary.



The average spend per full time equivalent employee appears to fall as the size of the business increases in this sector, with small-medium businesses averaging less than $275/FTE.

Analysing where small businesses are spending their limited resources, a third indicated some form of dedicated security technology (e.g. antivirus or a firewall) had been implemented in the previous year. 16% made improvements to their procedures, and 14% implemented some form of security training or awareness for their team. Just 7% conducted an external audit or review, such as a penetration test or vulnerability scan, with a similar number engaging a managed security service provider (MSSP).

The size and location of the business did not appear to influence the cyber fitness measures in which small businesses invested. While the scope of this study wasn't able to include what may cause one business to invest more in their cyber fitness than another, we were able to gain insight into the step(s) small businesses are contemplating and the help they may be seeking.

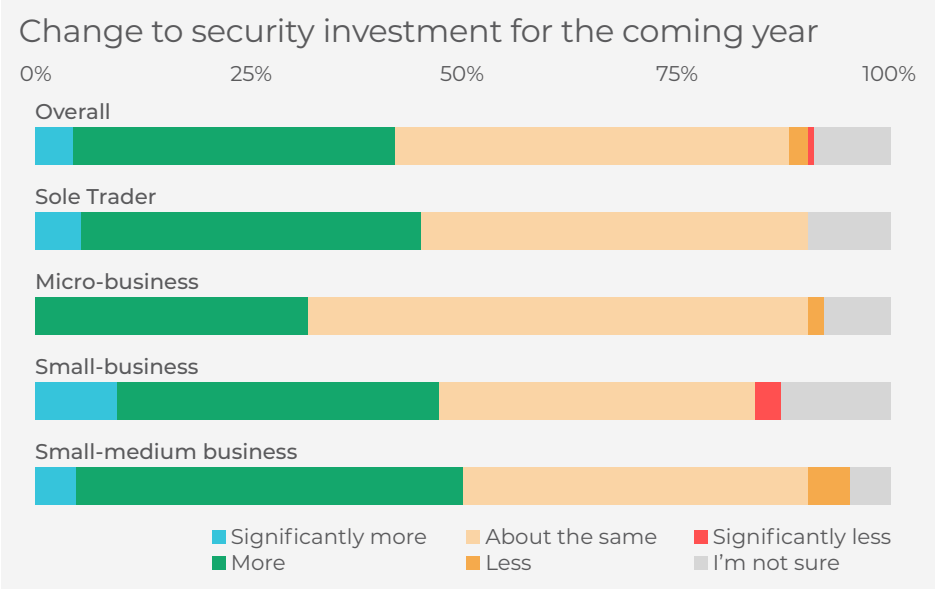
Small businesses do what they can, with what they have – but recognise that more needs to be done.

[12] 'The CISO Lens Benchmark 2020,' CISO Lens, retrieved 24 January 2021 from https://www.cisolens.com/benchmark

Planned investment in cyber fitness

Small business spend on cyber security may be low, but the vast majority (84%) expect to continue to invest in the coming year. **Around 40% of businesses expect to spend more** than they did in the previous year, suggesting a willingness to address the discomfort they are feeling.

This attitude was shared across businesses of all sizes and locations. However, it is likely that any additional cyber security funds would be reliant on how well the business is operating during a sustained global health crisis and economic downturn, which limits this area's growth unless external funding or compensation is available.



When forecasting investments for the coming year, it was promising to see a diverse mix of priorities. Importantly, procedure and behaviour improvements were prioritised much more closely to technology investment by respondents, suggesting an interest towards adopting a broader approach to cyber fitness among many small businesses.

Respondents suggested that external reviews and managed service providers should be playing a larger role in cyber fitness, yet both remain on the lower end of priorities. Small businesses don't see the value in paying to better understand their cyber risk, and are reluctant to pay a professional to manage it on their behalf.

Solutions that necessitate a significant upfront investment, direct engagement with an external provider and a focus on a subset of the problem space are unlikely to find traction among participants of this study. The muted results of the small business cyber security grant program fund[13] following the 2016 cyber security strategy is an indictment of such approaches in the small business segment.

[13] https://www.innovationaus.com/govt-missing-in-action-on-digital-smes/

There's no strong drive

Despite two in five small businesses having direct experience with a cyber incident, there's not a lot of external pressure on businesses to strengthen their resilience to cyber attack. Without government incentives or pressure from customers, few small businesses will be driven to work on their cyber security.

Remain alert, but not alarmed. Cyber attacks exploit the gaps in security that arise when small businesses are or become complacent. A cognitive challenge for cyber security defence is that when it's working well, you'll question why you need it in the first place. Don't fall for the trap!

Can automated cyber fitness health checks work?

While automated assessments are becoming more available, they are typically limited in scope to specific technical areas of cyber risk.

Traditional approaches to cyber risk assessment can take days, if not weeks; and often require specialists with expensive tools; the time and money required placing it well beyond the reach of small businesses. The Cynch Cyber Boot Camp was developed to work within these constraints to educate small businesses on their cyber risk coupled with simple steps to build their cyber fitness. Most businesses participating in the Cyber Boot Camp offered as part of this study completed an initial assessment of their cyber risk and began to **improve their cyber fitness within 15 minutes** of signing up. Over the course of the six week program, participating small businesses completed an average of 10 recommendations, finding just under 1 hour to work on their cyber fitness over the same period.

While seeing small businesses make gradual improvements to their cyber fitness was rewarding, it's notable that businesses that opted to pay for support from Cynch to optimise their engagement with the program invested more time, completing over the same period an average of 30 recommendations. The assessment technique and guidance provided was the same across both experiences, yet these results indicate there is significant benefit in small businesses having access to experts to answer their questions and give them confidence as they build their cyber fitness.

Influences on prioritisation

As anyone that has worked in a small business can tell you, there is never enough time or money to get everything done. Successful small business owners become masters of prioritisation, ensuring they and their teams are investing their resources effectively.

Only 1 in 10 small businesses found it easy to allocate time to work on cyber security, compared to 40% that have difficulty allocating time out of their week. This is more pronounced in metropolitan businesses, with 47% reporting trouble finding the time; while 33% of their regional counterparts reported the same. Time becomes less of a constraint as a business becomes larger, with 62% of small-medium businesses saying that time is neither difficult nor easy.

Few small businesses see the value in working with external suppliers to address their cyber risk, yet many struggle to find the time to manage things themselves. It's little wonder that gaps in cyber fitness persist.

What would make a business want to improve their cyber fitness?

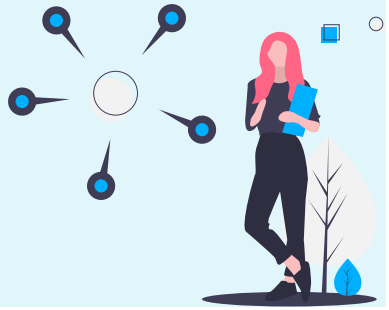
When asked what might influence a business to spend more time improving their cyber security, an active threat was flagged as the most influential. The other significant factor highlighted by respondents was the desire to have a better understanding of what could be done.

Internal constraints such as the inability to take action without support and affordability were factors that restricted the time spent on improving cyber fitness. Customer expectations and the potential for a competitive advantage were also noted, yet lower down than most internal factors.

Tailored cyber fitness

A clear theme that emerged throughout the study is a desire for targeted recommendations that speak to their specific circumstances. A key complaint about cyber.gov.au is that the information is too general, which makes it hard for study participants to apply to their own circumstances. Checklists and case studies focused on their industry and business size were suggested as one way to address this problem.

Small businesses don't expect personalised support from free sources like cyber.gov.au, but the generic approach is not working.



Recent changes to the Australian 2020 cyber security strategy present an opportunity to build cyber fitness of private businesses. However, as the lowest factor noted by respondents, increased board scrutiny is not a strong motivator for small businesses.

Expertise is out of reach

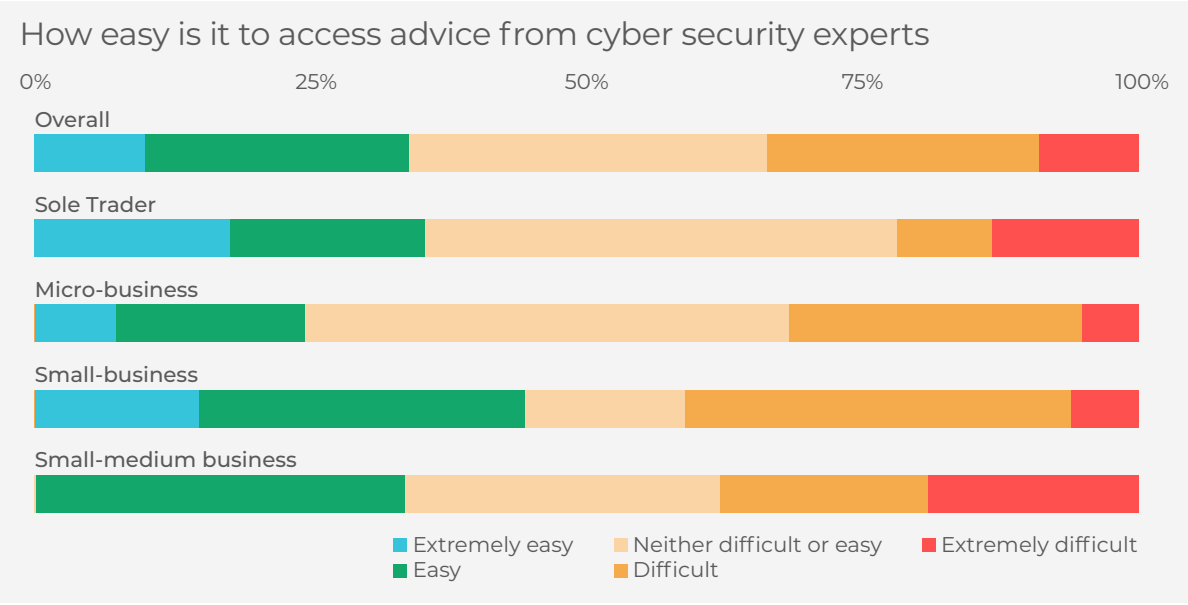
Small business owners are motivated, they're keen to learn and are used to wearing many hats to keep their livelihood afloat. It must be utterly deflating that, when they enquire about cyber security options for their business, they're pointed towards enterprise-level solutions with a price tag to match.

Look for a cyber security provider that understands how the world works for small – they're likely small themselves! The big guns may have top bidding on all the 'right' search terms to push the small players off the first page, but cyber security providers that cater specifically to small business needs are out there – finding them is a cinch.

Access to expertise

Research by AustCyber suggests that the cyber security skills shortage, especially with regards to technical skills, has improved[14] in recent years. This is a positive sign for the broader cyber security industry, however with few small businesses currently engaging cyber security professionals it's unlikely this shift has been felt in the small business sector.

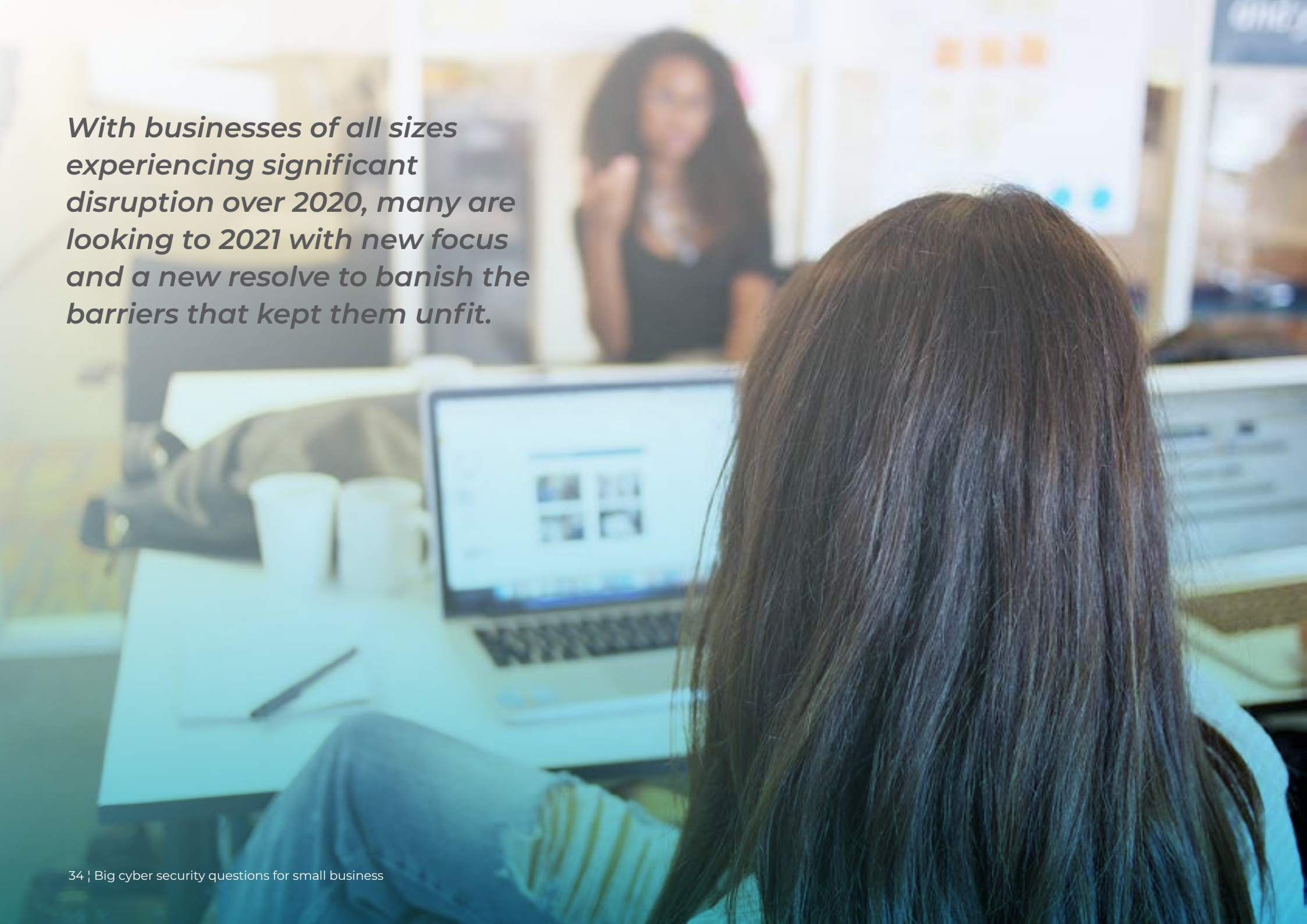
Confoundingly, when asked about the difficulty of engaging an external cyber security expert, an equal number found it easy, difficult and neither difficult or easy. Geographic location did not influence this perspective, however smaller businesses found accessing external expert advice more challenging than their larger peers.



[14] 'Australia's Cyber Security Sector Competitiveness Plan 2020,': Australian Cyber Security Growth Network, retrieved 24 January 2021 form https://austcyber.com/resource/australias-cyber-security-sector-competitiveness-plan-2020

The 2020 cyber security strategy focuses on helping small businesses improve their cyber fitness by working with larger corporates and associations. This approach is likely to raise awareness of cyber risk and solutions that are being embraced by small businesses, but without addressing gaps in technology, it's not likely that business processes and behaviour will advance.

The burgeoning small business market for cyber security services presents a number of opportunities for Australian providers. Those able to help small business owners understand the steps they can take to build cyber fitness packaged in simple, affordable solutions are likely to find success, particularly if outcomes can be achieved efficiently. The financial constraints of sole traders and micro businesses are likely to leave traditional security consulting out of reach for many, requiring innovative solutions such as the Cynch Cyber Boot Camp model to be developed to serve these needs.



With businesses of all sizes experiencing significant disruption over 2020, many are looking to 2021 with new focus and a new resolve to banish the barriers that kept them unfit.

Section 5: Conclusion

Help businesses understand cyber risks and responsibilities

Owners and those responsible for the cyber risks of small business must recognise the importance of managing cyber risk – and their own roles in building resilience into their business through cyber fitness. They've heard the warnings and guidance from government and industry, and want to learn about their cyber risk. Give it to them straight, from a place of shared understanding that respects their intelligence, and you'll create a passionate brand supporter for life.

Speak plainly, avoid jargon

Cyber security is a complex problem space. The technical language used can add to confusion for small businesses who are already struggling to wrap their heads around risks relevant to their specific circumstances. When provided relevant, plain-language guidance, small businesses readily embrace recommendations, albeit at a pace and cost relative to their size.

Keep small budgets in mind

The majority of small businesses plan to maintain or increase their investment in the cyber fitness of their business. They recognise the need to look beyond technical solutions when addressing their risks, and they'll gladly embrace solutions from a cyber security provider if that provider offers realistic packages for tomorrow's big spender today.

Encourage war stories – and wins – to be shared

Direct experience with a cyber attack is still a primary motivator for action, however many small businesses would do more if they understood what could be done and could do themselves within budget. Positive external influences, such as increased expectations from customers and an opportunity to create a competitive advantage, are not currently strong motivators for small businesses but are still worth monitoring as the market matures.

Offer expertise that's within reach of small businesses

Small businesses weren't interested in engaging external cyber security expertise to better understand and manage cyber risk. Those that did were soon dismayed by packages targeted towards larger businesses, priced out of contention and for a sophistication well above the requirements of their small business network.

Cynch is dedicated to improving the cyber security of Australian small businesses. If you're interested in cyber security or cyber fitness, we'd love to hear from you.

The Cyber Boot Camp class of '21 is closing soon.

Get started on your cyber fitness today.

Simplify and share solutions

There's a fundamental disconnect between the idea of a virtual international spy gaining entry to your online livelihood and the limp meh that's elicited from those responsible for common cyber security. Threat awareness and guidance towards basic cyber security measures to mitigate them is likely to grow as government and industry support programs are expanded. Without support to identify and take more specific steps and simpler, more affordable solutions entering the market the small business sector is likely to continue underinvesting in their cyber fitness.

Australian small businesses have demonstrated resilience through recent trying times, in no small part as a result of accelerated digital adoption to enable teams to work remotely and offer services online. As the Australian economy recovers, the future of small business is unlikely to resemble that of the past. Innovative solutions designed to help small business owners understand their cyber risk and prioritise their limited resources will play a critical role in realising the cyber fit future Australia deserves.

For further information contact

Cynch Security
710 Collins Street, Docklands Vic 3001
hello@cynch.com.au