CyberWardens.

Building a culture of cyber safety in Australian small businesses

Cyber Wardens Research Report

March 2024

COSBOA COUNCIL OF SMALL BUSINESS ORGANISATIONS AUSTRALIA

About Cyber Wardens

At Cyber Wardens, we are working to ensure Australia's 2.5 million small businesses operate in a cyber-safe environment, as online scams and fraud continue to rise.

The program builds a culture of cyber safety and creates cyber skills within Australian small businesses. Launched in November 2023, the program will train 50,000 Cyber Wardens over the next three years.

The Cyber Wardens eLearning training course takes just 45 minutes to complete on any device, is free to all Australian small businesses, and employees don't have to be tech-savvy or an information technology (IT) wizard to understand it.

Cyber Wardens training is led by expert advice and research from the Australian small business community. Cyber Wardens training can help you defend against digital break-ins and keep cyber criminals out of your business. For example, by installing multi-factor authentication, you set a virtual alarm to keep your business safe.

Cyber Wardens can educate and support their colleagues about cyber safety risks and give them the tools and skills they need to help detect and ward off cyber attacks together. There is strength in numbers when upskilling your workforce to protect your small business as a team.

Cyber Wardens is an initiative of the Council of Small Business Organisations of Australia (COSBOA), supported by the Australian Government and an industry alliance led by Telstra, CommBank and the Australian Cyber Security Centre.

TABLE OF CONTENTS

We acknowledge the Traditional Owners of Country throughout Australia. We pay our respects to Elders past, present and emerging and celebrate the diversity of Aboriginal and Torres Strait Islander peoples and their ongoing culture and connection to lands, waters and skies.

CEO Foreword

Australian small businesses face cyber security threats every day. Yet many owners, CEOs and employees don't believe their small business could be a target. The belief that being small makes you safe is a fallacy.

Recent data released by the Australian Signals Directorate clearly shows the frequency and financial impact of the threat is rising, as cyber criminals are increasingly targeting Australian small businesses.

Knowing a problem exists isn't enough to solve it. We need a cultural shift and targeted support. To embed a culture of cyber security into Australian small businesses, we need to know what can drive this cultural change.

Just as we physically protect ourselves by locking up our businesses and homes at night, small businesses need to understand how and why they should lock their digital doors.

COSBOA, through Cyber Wardens, has completed the first year of an in-depth research project to measure and map small business cyber security behaviours and attitudes. This qualitative and quantitative research included almost 2,100 small businesses across Australia.

From this evidence, we uncovered five attitudinal and behavioural segments based on small businesses' attitudes, concerns, awareness and behaviours relating to cyber security.

The factors that drive the cyber maturity of a small business are far more complex than the size, age or type of business.

Small businesses vary considerably in their awareness, level of concern, and preparedness to respond to cyber threats. Some businesses are leading the way by thinking and talking regularly about cyber security and embedding it in their day-to-day operations. However many small businesses are unaware of their vulnerability and are yet to take steps to protect themselves.

This research is the first step in understanding what small businesses need to do, what might be standing in their way and what we can do to support them. The research also helps us in our national delivery of the Cyber Wardens program. Since the launch in November 2023, we have made a strong start to our aim of training 50,000 Cyber Wardens across Australia over the next three years.

The Cyber Wardens program is the vehicle for this national cultural change and supports the technical uplift needed to protect Australian small businesses from evolving and increased cyber threats.

Luke Achterstraat

COSBOA Chief Executive Officer

1. Research overview

COSBOA, through Cyber Wardens, completed the first year of a multi-year research project to measure and map small business cyber security behaviours and attitudes.

This new research builds on past work conducted by COSBOA through Cyber Wardens, including 'Small Business Cyber Security Research Report 2022' and 'Understanding Small Business and Cyber Security 2023', to understand the barriers and drivers of action that can encourage or prevent small businesses from increasing their cyber security posture.

We investigated attitudes and mindsets, organisational culture, cyber posture and technical skills, and everyday business cyber-safe habits to comprehensively understand cultural and technical competencies across the small business sector.

The qualitative and quantitative research, from late 2023 and early 2024 engaging small business owners and their employees, comprised of:

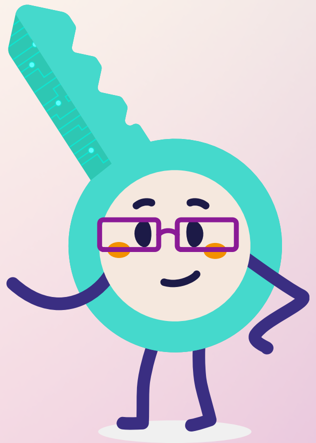
- a deep dive into small business cyber security barriers and attitudes using eight focus groups;
- a national survey of 2,098 people (small business owners/employees); and
- 15 in-depth interviews.

These participating small business owners and employees represent a broad range of industries and business types across different metropolitan, regional and rural locations. It included men, women and non-binary people across a broad age range working in a variety of roles and with varying levels of cyber security awareness and experience.

For the national small business survey, we set quotas to ensure a reliable sample of each business size: sole traders, micro-businesses, small businesses with 5–9 employees, small businesses with 10–14 employees and small businesses with 15–19 employees. This data is unweighted.

The results highlight the critical importance of building a cyber-safe culture among small business alongside, and even ahead of, increasing their technical cyber security measures.

The research was conducted in partnership with 89 Degrees East.



1.1. Research participants snapshot: Small business cyber security research

Qualitative Sample

8 Focus Groups

45 Small Business Owners

15 Depth Interviews

4 Small Business Owners

6 Sole Traders

5 Employees

Quantitative Sample

Business Types

2,098 Businesses

416 Sole traders

481 Micro businesses

1,192 Small businesses

Role

639 Owners

1,043 Employees

Gender

57% Female

42% Male

1% Non binary

Geography

72% Metro

28% Regional

Age

18-24 years	6%
25-34 years	22%
35-44 years	24%
45-54 years	18%
55-64 years	16%
65+ years	13%

Years of business operation	
less than 1 year	5%
1–5 years	30%
6–10 years	25%
11–20 years	21%
21 years or more	19%

Type of business	
Family business	25%
Side hustle	8%
Start up	15%
Scale up	14%
Home-based business	13%
Maturity stage	34%

Business industry	
Business or administration services, consulting, finance, insurance	16%
Retail or clothing and accessories	13%
Food or drinks production, catering, cafes, and restaurants	11%
Construction, manual, and building industry	11%
Personal care, beauty, and well-being	4%
Education, training, and childcare	5%
Healthcare, caring, and support services	9%
Arts and entertainment	4%
Manufacturing	4%
Information technology products and services	4%
Transport or delivery services, logistics and supply chain, import, export, or wholesale	4%
Other	14%

2. The fallacy of 'small and safe'

2.1. Australian small businesses are under threat

Australia's 2.3 million small businesses are the heartbeat of Australia's national economy. Small business is our largest employer, representing 5 million people and contributing $418 billion to Australia's GDP.[1]

While the online ecosystem presents many opportunities for small businesses to innovate and grow, it also elevates the risk of a cyber attack. Data released by the Australian Cyber Security Centre (ACSC) clearly shows the frequency and impact of the threat to Australian small businesses is rising, as cyber criminals are increasingly targeting Australian small businesses.

Over 8 in 10 (81%) small business owners/CEOs and employees have experienced a cyber threat at work and/or in their personal lives.

[1] Australian Small Business and Family Enterprise Ombudsman (ASBFEO)

Despite the serious rate of attacks, our research reveals that many small businesses consider themselves too small to be targeted by cyber crime.

Attacks are increasing in cost and frequency[2]

$46,000 per attack

Average cost to a small business of cyber crime per report

Every 6 minutes

A cyber crime is reported in Australia, increased 23% in 2023

[2] ASD Cyber Threat Report 2022–2023

7 in 10 (70%) have received a suspicious SMS, email or phone call, making this by far **the most common cyber threat.**

2 in 10 have been exposed to an **invoice or payment scam** (21%).

2 in 10 have been exposed to **a marketplace scam** (20%).

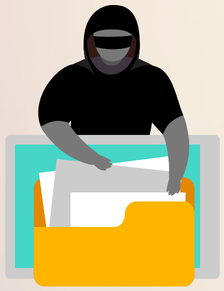
17% have had their data leaked due to an attack on another organisation, and 10% have experienced **having their passwords or accounts hacked.**

Less than 1 in 10 (6%) reported experiencing a malware **or ransomware attack.**

Small business threats: Top three reported cyber crimes[3]

1. Inbox break-ins

Email compromise attacks are like a break-in in your inbox. Once inside, cyber criminals gain access to critical information and can launch more damaging attacks.



2. Fake invoices and payment redirection scams

Business email compromise (BEC) fraud is a type of scam to trick you out of money or goods, usually by sending fake invoices that redirect payments to hackers.

3. Banking burglary

Online banking fraud allows cyber criminals to access your bank accounts and transfer your hard-earned cash.

2.2. What you don't know can hurt you

A limited understanding of the frequency and significant impact of cyber attacks is holding small businesses back from protecting themselves.

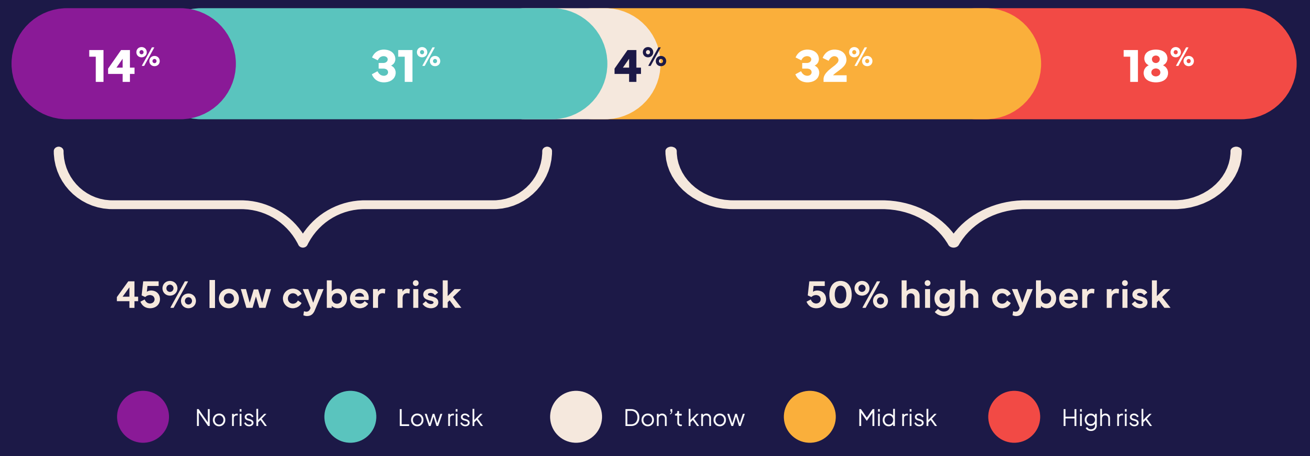
Our small business research reveals that while cyber security is among the top three risks for small businesses (third highest risk after energy prices (54%) and cost of staff (52%)), nearly half of small businesses believe cyber security threats pose no risk (14%) or are only a low risk (31%) to their business in the next five years.

The reality for small to medium businesses is quite different. In 2020, 43% of cyber attacks in Australia targeted small to medium businesses.[4]

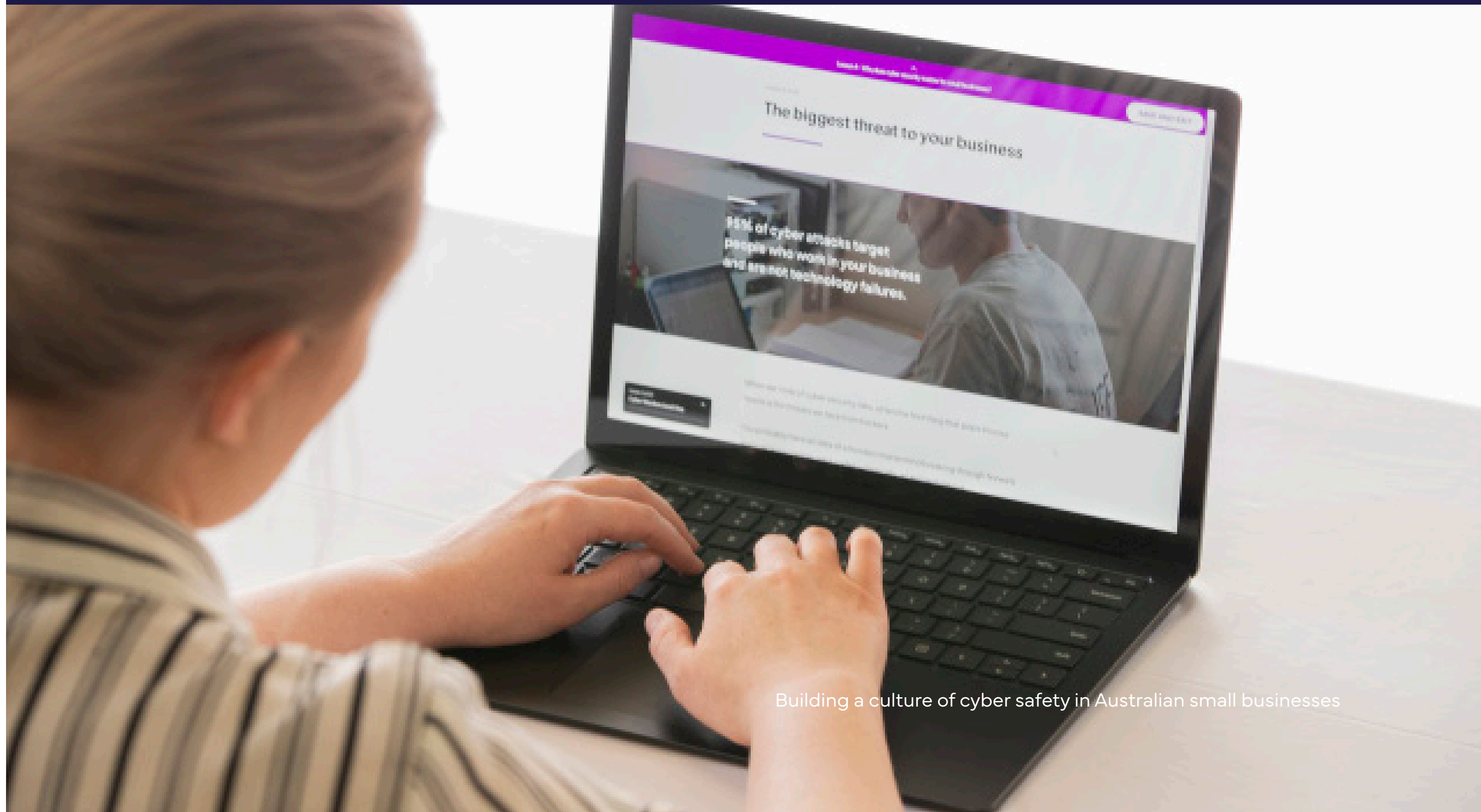
The majority of small businesses (61%) are not talking about cyber security regularly, and this further increases the risk they face.

Small businesses that demonstrate the lowest cyber maturity are among the least concerned about the threat of cyber security, emphasising that small businesses aren't motivated to protect themselves from threats they don't see or understand.

Perception of cyber risk



Question: Thinking about the next five years, to what extent do the following pose a threat to your business? (Cyber threats)


The biggest threat to your business
95% of cyber attacks target people who work in your business and are not technology failures.

[3] Ibid.
[4] Australian Cyber Security Centre, 2020

2.3. Cyber reality check: The little fish mentality

While awareness about cyber attacks on large companies is growing, many small businesses continue to underestimate their vulnerability. Only a third (35%) of small business owners/CEOs and employees feel vulnerable to attack due to being a small business.

> “Cyber threats wouldn’t be very prevalent in small businesses because there’s no real incentive for the hackers. If you’re looking for money, there’s bigger fish to fry than little businesses.”
>
> Sole trader — psychologist
> (man, 40, metro TAS)

> “I’m just a little person, what would they want to attack me for? When they can attack big companies and get quite a lot of money? Maybe if I had a big organisation with a lot of employees using the internet, maybe I would be a target because I don’t know what websites they’ve been on but I’m not concerned about the risk of a cyber attack on my business, because it’s just too small.”
>
> Micro business owner — hairdressing salon
> (woman, 62, metro VIC)

It’s common for small businesses, particularly sole traders and micro businesses in the least cyber-safe segments, to see themselves as “little fish” who don’t have much to offer in terms of finances or valuable business information. Many assume cyber criminals would gain much more from hacking a larger company, giving them a false sense of security.

Four in 10 (38%) small businesses still think it’s much more important for medium and larger businesses to practice cyber security than it is for small businesses, and a further 3 in 10 (28%) are on the fence about this. Even among small businesses that see the logic in cyber criminals targeting less secure small businesses, there is still disbelief that *their* business could be a target.

> “I wouldn’t think my business would be a target. I suppose I see myself as such a little fish. I’m sure there’d be a shark that would be meatier and would be able to provide cyber criminals with a lot more.”
>
> Sole trader — mental health practitioner
> (woman, 59, regional VIC)

> “I don’t believe my small business will be on anyone’s radar to try and extract any income out of me. My turnover is not enough to be a target. I’m not a big enough player and I don’t store customer details or payment information, all that is stored via a third party.”
>
> Sole trader — e-commerce
> (man, 39, regional QLD)

> “I think we feel we’re not that big of a target, so that’s why we haven’t done more than what we have. There are bigger businesses out there doing far more volume and far more transactions.”
>
> Micro business director — wholesale electrical supplies (man, 62, metro NSW)

> “I’ve come to terms with the fact a cyber attack will probably happen at some point, but you never think it’s going to happen tomorrow.”
>
> Micro business owner — agricultural services
> (man, 40, regional NSW)

2.4. Major attacks reinforce ‘too small to target’ perceptions

Even though 7 in 10 (67%) small business owners/CEOs and employees report major cyber attacks on big companies have made them think more about cyber security, awareness of big companies being targeted isn’t necessarily translating into small businesses doing more to protect themselves.

Rather, high-profile attacks may reinforce the view that big businesses are the more likely targets of cyber attacks.

> “On the whole, you don’t really hear much about cyber attacks. I mean, we hear about Optus, but it’s not something I would consider a daily occurrence, and maybe it should be and maybe we just need to know that small businesses get attacked every single day.”
>
> Micro business owner — manufacturing
> (man, 54, regional QLD)

> “I don’t think it [cyber security] is a major problem for small businesses. Because just look at the low value for the hackers or whoever is trying to get in. I can see the value in hacking bigger organisations like the telecommunications companies, the banks, and even government but I’ve had very little communication with people in my size of business, other sole traders, that have been impacted.”
>
> Sole trader — sports consultant
> (man, 66, metro QLD)

2.5. Small businesses are reliant on 'Security-by-Design' reforms

Secure-by-Design is a proactive approach to enhance cyber security as a core product feature, to ensure consumers are protected. The primary aim is to safeguard consumer privacy and data by creating products with fewer vulnerabilities, prioritising security throughout the entire development process.

Overall, the low perception of cyber risk and passive approach to implementing cyber security measures amongst many small businesses highlight the importance of 'cyber security by design' reforms to support and protect Australian small businesses and their customers.

Concerningly, many small businesses are relying heavily on the security of platforms they use every day assuming a 'secure-by-design' software ecosystem already protects them. They assume that the sophistication and dependability of the systems put in place by software companies are far beyond what they could achieve in their small business, so it's best to leave it up to them. Research suggests the vast majority of cyber attacks in Australia involve human error.

> "My assumption is that the software or provider that I am putting my faith in has kept everything up to date so that it's not accessible to hackers."
>
> Sole trader — mental health practitioner (woman, 59, regional VIC)

> "My third-party providers have paid millions of dollars to have that security."
>
> Sole trader — e-commerce (man, 39, regional QLD)

> "You've got to trust software and systems to a degree. Nothing is ever going to be 100%, nothing is guaranteed in life… you just hope an attack doesn't happen to you."
>
> Micro business co-owner — skincare retail (woman, 53, metro VIC)

3. Benchmarking cyber safety basics

3.1. Gaps in basic cyber safety create significant vulnerability

Cyber Wardens training builds small business skills across cyber security fundamentals:

- multi-factor authentication
- strong password management
- automatic software updates, and
- ensuring effective backups to support recovery.

These foundational cyber security measures offer a reasonable level of protection against common attacks faced by small businesses. However, for most small businesses, these four critical safety measures are not effectively implemented, leaving them vulnerable to serious cyber attacks.

3.2. Multi-factor authentication absent in 50% of small business cyber defences

One of the most effective ways to protect online accounts and applications from cyber criminals is through multi-factor authentication (MFA), a two-step verification to verify a user's identity and prevent unauthorised access.

Just like a password is a key to unlocking a business, MFA represents an additional layer of security like a digital alarm system. This powerful strategy can help keep hackers and criminals out of important business accounts, yet only one in two small businesses are implementing this powerful strategy.

3.2.1. Financial accounts most likely to be protected with MFA

Small businesses are most likely to utilise MFA on their financial accounts, where MFA is often enforced by their financial institution, compared to other important business accounts such as cloud drives and email, where users themselves are likely to store and maintain sensitive business information.

Only 1 in 2 small businesses have their cloud drives and social media accounts protected with MFA. A particular concern is the significant drop in small businesses protecting their email accounts with MFA, given that business email compromise (BEC) and BEC fraud are two of the top three cyber crimes directed at small businesses in 2023, according to the ACSC.

57% of small businesses are protecting their **financial services** accounts with MFA

50% of small businesses are protecting their **cloud and social media** accounts with MFA

46% of small businesses are protecting their **email** accounts with MFA

3.3. Weak password management increases vulnerability

3.3.1. Sharing passwords is common practice

Sharing passwords between employees or allowing team members to access shared passwords through a password document is common practice in small businesses with more than one employee.

Only 5 in 10 (52%) ensure not to store passwords in one place, e.g. making passwords accessible to team members through a central password document.

Only 6 in 10 (61%) currently provide each employee with their own login and password. Previous research conducted by Cyber Wardens found this risk to be pronounced among casualised workforces.

3.3.2. Applying advanced password strategies

Few small businesses have a sophisticated approach to password management. Only 3 in 10 apply advanced password management strategies, including using an encrypted password management system or strengthening passwords by upgrading to passphrases.

30% of smal businesses have upgraded passwords to **passphrases**

34% of smal businesses use encrypted **Password Management Systems**

3.4. Half of small businesses lag in software patching efforts

When your software is not up to date, it's like leaving the doors to your business unlocked. One in two (52%) small businesses are keeping their digital doors locked by ensuring software vulnerabilities are patched through automatic software updates on computers and devices.

However, everyday 'bad habits' undermine their patching efforts. More than 1 in 4 (27%) put their computers in 'sleep mode' rather than shutting them down, which may prevent software updates from installing, and about 1 in 5 (18%) 'snooze' software updates.

Only 2 in 5 (42%) small businesses report old software is deleted and uninstalled on company devices. Small businesses are less likely to report patching the operating system of additional hardware, such as point-of-sale terminals, within two days of a software update, with only 37% reporting this practice.

3.5. Only 1 in 2 small businesses are backing up daily

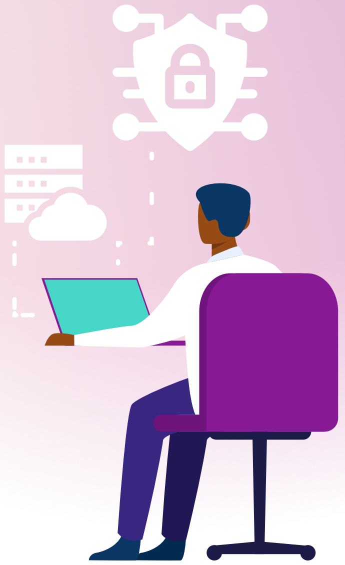
Strong and secure backups are essential to cyber resilience. Without them, the ability of small businesses to recover from a cyber attack is compromised.

While 6 in 10 (60%) small businesses have taken steps to protect data and important business systems, only 5 in 10 have a backup system to help recover from a cyber attack (50%) and are backing up important information securely each day (53%).

3.6. Beyond the basics and towards the 'Essential 8'

Beyond the fundamentals of backups, password management, software patching and multi-factor authentication, the Australian Signals Directorate (ASD) Essential 8 mitigation strategies provide a useful framework for benchmarking more advanced cyber security practices. The following small business behaviours demonstrate that small businesses have a significant way to go in applying advanced Essential 8 practices such as application hardening, restricting administrative privileges, application control and hardening, and restricting macros.

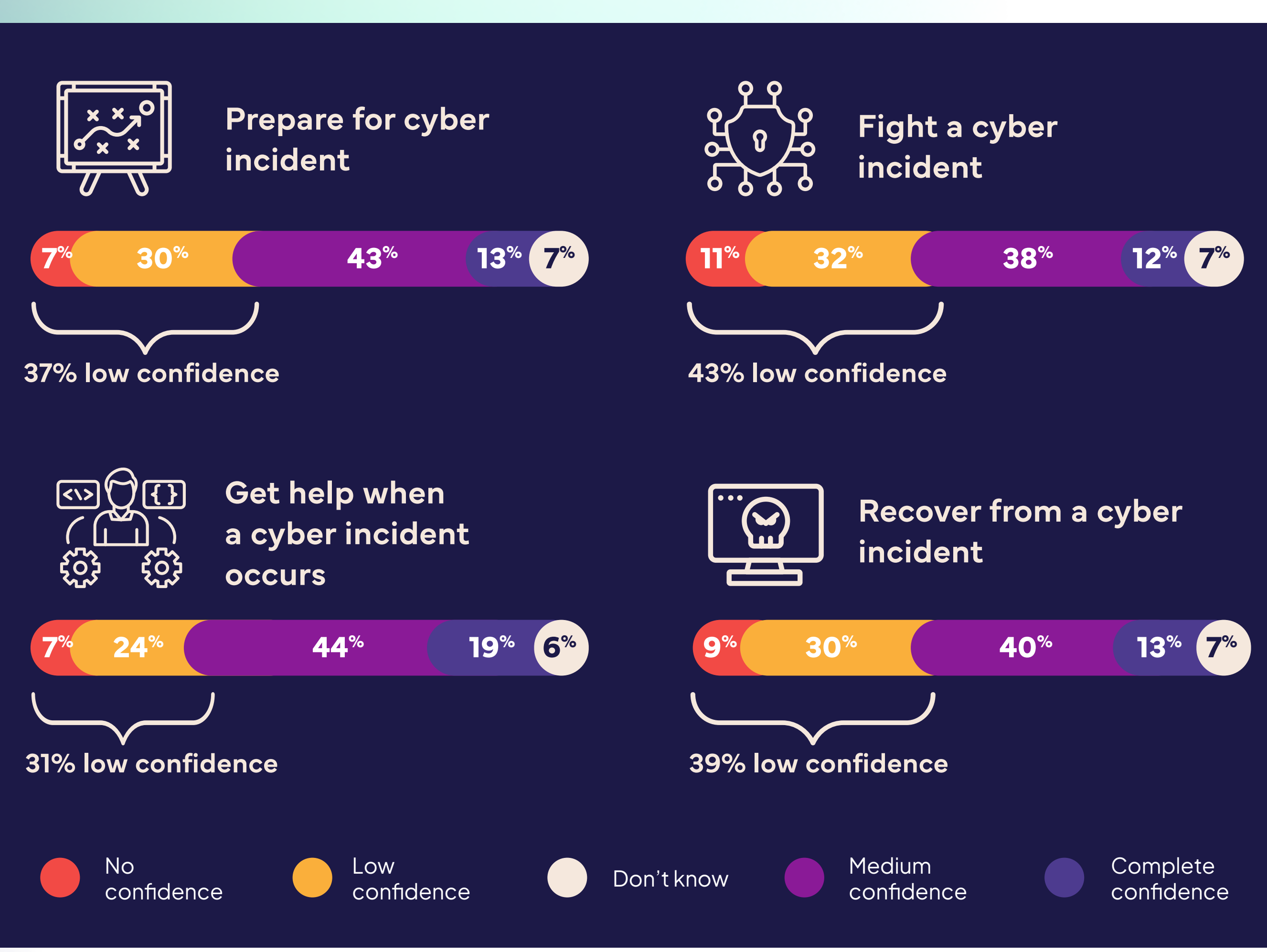
- 47% have new computers, phones or technology devices set up by an IT expert and configured for security (application hardening).
- 43% restrict administrative privileges and report employees are given access to specific software features needed to do their job, not the entire system (for important business software, databases and business social media accounts).
- 37% set business rules that limit the applications and software that are allowed on company devices such as laptops and phones (application control).
- 38% report that staff receive training about cyber security and how to protect the business from cyber threats.
- 37% set business rules within apps and software to limit what they can do (application hardening).
- 25% of small businesses ensure Microsoft macros (automation scripts) are configured for security (restricting macros).



3.7. At every part of the journey small businesses lack confidence

Many small businesses are unprepared to respond to cyber threats. On average, 4 in 10 small businesses have little to no confidence in their ability to:

- Prepare for a cyber incident (37% no confidence or low confidence)
- Fight a cyber incident (43% no confidence or low confidence)
- Know where to get help when a cyber incident occurs (31% no confidence or low confidence)
- Recover from a cyber incident (40% no confidence or low confidence)



Small businesses remain uninsured despite growing cyber threats

Fewer than 1 in 4 (24%) small businesses have specialised cyber insurance protection despite a 23% increase in reported cyber attacks in the past 12 months.

4. Research-informed segmentation

4.1. The overarching questions

What are the cyber safety attitudes and beliefs of Australian small businesses?

What factors are driving the small business approach to cyber security?

These questions drove the design of this research project to discover how to build urgency and develop cyber-safe cultural competencies and technical know-how in Australian small businesses. Traditional factors like business size or age of the business had minimal impact on a business's preparedness to deal with cyber threats.

The frequency of workplace conversations about cyber security was the driving factor that correlated with small businesses demonstrating an increasing cyber maturity. Building a culture of cyber safety helps drive an uplift in cyber-security behaviours.

From the research, we developed five attitudinal and behavioural segments based on small businesses' attitudes, concerns, awareness and behaviours relating to cyber security.

Unaware & Inactive	Passive & Foundational	Aware & Emergent	Attentive & Maturing	Ready & Resilient

4.1. Factors of the segments

Attitudes and mindset

- Attitudes towards cyber safety
- Perceived level of cyber-security risk
- Confidence in the ability to manage a cyber incident

Organisational culture

- Cyber-safe workplace culture
- Cyber security training
- Frequency of workplace conversations

Cyber posture and technical skills

- Demonstrated behaviour of implementing cyber fundamentals
- Sophisticated cyber-safe practices in place

Bad habits

- Everyday business habits are undermining cyber-security posture

4.2. Topline findings by segment

To enhance cyber security awareness and urgency among small businesses, a tailored approach is critical. This segmentation model has been created to effectively reach and communicate with small businesses. The segmentation offers insights into the diverse stages of maturity within small businesses' cyber security journeys, providing a detailed understanding of each segment's demographics, attitudes, behaviours, priorities, and barriers to prioritising cyber safety.

	Research identified segments				
	Unaware & Inactive	Passive & Foundational	Aware & Emergent	Attentive & Maturing	Ready & Resilient
Cyber maturity	Low	Low Emerging	Emerging	Developing	Mature
Cyber risk perception	Low	Moderate	High	High	Managed
Cyber safety conversations	Rare	Rare	Often	Regular	Regular
Cyber-safe workplace culture	Non-existent	Non-existent	Early Stage	Developing	Established
Cyber training	Low	Low Emergent	Emerging	Developing	Consistent
Foundational cyber practices	Few	Emerging	Emerging	Developing	Consistent
Sophisticated cyber practices	Very Few	Low Emerging	Emerging	Developing	Consistent
Cyber resilience	Low	Low Emerging	Emerging	Developing	Mature

4.2.1 Cyber-safe mindset drives behavioural change

The most cyber-safe small businesses have a cyber-safe outlook and are intentional in their approach to cyber security. They think and talk about cyber security regularly and see it as everyone's responsibility. They also dedicate resources and embed cyber security into day-to-day operations. The previous table demonstrates how the two most mature segments, the Attentive & Maturing and the Ready & Resilient, have much stronger cyber-safe practices in place, largely shaped by **their cyber-safe mindset.**

In the least cyber-safe segments, cyber security is not front of mind. They are not thinking or talking much about cyber security, and do not have a culture of cyber safety.

Only when the cyber-safe mindset develops, do we see the 'Aware & Emergent' segment make an intentional shift towards increased cyber security. This is facilitated by a stronger understanding of risk and a regular cadence of conversations about cyber security, demonstrating cyber safety is top of mind.

Until their mindset changes, it is unlikely small businesses in these segments will progress to become more cyber safe. Building a culture of cyber safety is anchored in regular workplace conversations about cyber security and is essential in supporting small businesses to implement cyber-safe practices.

5. Small business segments inform the cyber security journey

5.1. Unaware & Inactive

Small businesses in the Unaware & Inactive segment are highly unconcerned about cyber threats and are often not thinking or talking about cyber security at all. These businesses have minimal cyber-safe practices in place, are not providing cyber security training, and do not have a culture of cyber safety.

The Unaware & Inactive regularly practice bad online habits (such as ignoring system update prompts), and they are more likely to see cyber security as someone else's responsibility. Most have shallow confidence in their ability to prepare for and respond to cyber threats.

In short, small businesses in this segment are **unaware** of cyber threats and don't see themselves as a target. As a result, they are **inactive** when it comes to protecting their business.

Sole traders, side hustles, home-based businesses and businesses that have been operating for less than a year are overrepresented in this segment, as are people with casual work arrangements.

Unaware & Inactive	
%	44% of sample
Estimated #	
Sole Traders	990K
Micro Businesses	300K
Smalll Businesses	90K

Unaware & Inactive under index for all of the risks/threats

Maturity Index	**Least** mature
Cyber threat perception	**Not thinking or talking** about cyber security
Confidence	**Very low confidence** in their ability to prepare for and respond to cyber threats
Awareness	**Low awareness** of cyber threats and how to be cyber safe
Cyber-safe practices	**Minimal** cyber-safe practices in place
Cyber-safe culture	**Non-existent culture** of cyber safety
Training	Very **unlikely** to be providing cyber security training
Bad habits	**'Bad habits'** are a regular occurrence (though likely underreported due to low awareness)

Cyber skillset	Cyber mindset
Not practising cyber safety On average, fewer than 3 in 10 businesses in this segment have basic cyber-safe practices in place. They are most likely to have unique logins for employees (39%) and least likely to use passphrases (14%) or an encrypted password management system (16%).	**Cyber security is far from front of mind** Cyber security is not on the radar of many small businesses in this segment. They have the lowest awareness and concern of any segment. 7 in 10 are not at all concerned (31%) or are only a bit concerned (37%) about the risk of a cyber attack impacting their small business.
Cyber security training is rare Only 1 in 10 (10%) in this segment say staff receive training about how to protect the business from cyber threats.	**Not thinking or talking about it** 53% can't recall a time cyber security has been discussed in the workplace, and only 17% discuss it monthly or more often.
Not prepared for an attack 5 in 10, on average, have no or low confidence in their ability to fight a cyber attack (54%), recover from a cyber attack (49%) or know where to get help if a cyber attack occurred (45%).	**Don't see themselves in cyber safety** This segment are the least likely to believe it makes a difference when they, as an individual, practice cyber-safe habits (only 50% agree). They are also least likely to think everyone plays a role in cyber security, not just IT experts (only 61% agree).

The opportunity to be more cyber safe is greatest with this segment

The Unaware & Inactive segment is the largest cohort. Unaware & Inactive therefore present the greatest risk, as they are the least mature on their cyber security journey and make up the greatest number of small businesses.

The key objectives for the Unaware & Inactive segment are to:

- increase awareness of cyber risk
- reinforce with sector leaders and industry advocates the size of the Unaware & Inactive market and the importance of 'security-by-design measures'.

5.2. Passive & Foundational

Small businesses in the Passive & Foundational segment have some basic cyber-safe practices but are not actively thinking or talking about cyber security.

'Bad habits' are still occurring in these small businesses and they have low confidence in their ability to identify and respond to cyber threats.

This segment's **passive** approach to cyber security is a product of their limited awareness and lower levels of concern about cyber threats. Despite the **foundational** practices they have in place, businesses in this segment are not thinking or talking about cyber security and are unlikely to take further steps to protect themselves unprompted.

Overrepresented small business cohorts include sole traders, small businesses in their maturity stage and those operating for 21 years or longer.

Passive & Foundational	
%	16% of sample
Estimated #	
Sole Traders	310K
Micro Businesses	110K
Smalll Businesses	30K

Maturity Index	Low
Cyber threat perception	**Not thinking or talking** about cyber security
Confidence	**Low confidence** in their ability to prepare for and respond to cyber threats
Awareness	**Moderate awareness** of cyber threats and how to be cyber safe
Cyber-safe practices	**Some** cyber-safe practices in place
Cyber-safe culture	**Non-existent culture** of cyber safety
Training	**Neither more likely or less likely** to be providing cyber security training
Bad habits	**'Bad habits'** are occurring

Cyber skillset	Cyber mindset
Have basic cyber-safe measures in place More than half have some basic cyber-safe practices in place. These include automatic software updates (63%), multi-factor authentication on financial accounts (70%), daily back-ups (72%) and unique passwords and logins for team members (64%).	**Cyber security is not front of mind** 5 in 10 (48%) are discussing cyber security a few times a year, but only 23% discuss it monthly or more often. Less than a third (27%) are considering cyber security when making business decisions.
Not confident to respond to threats Many have no or low confidence in their ability to prepare for (39%), fight (49%) and recover from a cyber incident (42%), though they are more confident about where to get help if an attack did take place (71% were confident about this).	**Not very concerned or aware of threats** More than half (54%) are not at all concerned or are only a bit concerned about the risk of a cyber attack impacting their small business.
Few are training staff to protect the business Only a quarter (25%) of small businesses in this segment report staff receive cyber security training to protect the business from cyber threats.	**Open to everyone playing a role in cyber security** Compared to the Unaware & Inactive, this segment are more likely to believe it makes a difference when they, as individuals, practice cyber-safe habits (74% agree) and to see cyber security as something everyone plays a role in, not just IT (79% agree).

Building awareness is key to cultivating a cyber-safe mindset in this segment

The key objective for the Passive & Foundational segment is to:

- use the awareness and education campaign to move this segment up to Aware & Emergent.

5.3. Aware & Emergent

Small businesses in the Aware & Emergent segment are in the early stages of their cyber security journey.

They are talking about cyber security regularly but don't yet have a consistent culture of cyber safety. They are concerned about cyber security threats but only have a few basic cyber-safe practices in place — along with a number of 'bad habits'.

Few Aware & Emergent small businesses are conducting cyber security training and they are not overly confident in their preparedness to respond to cyber threats.

While many in this segment still view cyber security as complicated and time-consuming, they do think cyber security is important and see the value in cultivating a culture of cyber safety.

This 'middle' segment's **awareness** of risks and frequency of conversations about cyber security differentiates them from less mature segments. Where they differ from the more mature segments is in their **emerging** cyber safe culture and practices. This segment has potential to become more cyber safe with the right tools and support.

Several small business cohorts are overrepresented in this segment, including family businesses, start ups, small businesses with more employees (10 to 19) and businesses with a physical office.

Aware & Emergent	
%	13% of sample
Estimated #	
Micro Businesses	100K
Smalll Businesses	40K

Note: Sole traders are underrepresented in this segment. A key criterion used to distinguish Aware & Emergent from the Passive & Foundational segment is whether they are talking about cyber security regularly. In the first year of the small business survey, this meant sole traders (who have no one else in their business to 'talk to') were inadvertently excluded. In future surveys, this will be expanded to include sole traders who are thinking regularly about cyber security.

Maturity Index	Emergent
Cyber threat perception	**Thinking and talking** about cyber security regularly
Confidence	**Moderate confidence** in their ability to prepare for and respond to cyber threats
Awareness	**High awareness** of cyber threats and how to be cyber safe
Cyber-safe practices	**Some** cyber-safe practices in place
Cyber-safe culture	**Developing culture** of cyber safety
Training	**Slightly more likely** to be providing cyber security training
Bad habits	**'Bad habits'** are less than average

Cyber skillset	Cyber mindset
Basic cyber-safe practices On average, 5 in 10 Aware & Emergent small businesses have basic cyber-safe practices in place, including automatic updates (53%), daily backups (49%), and use of MFA on company accounts - financial (55%), email (48%) and cloud and social media (46%). Advanced cyber-safe practices are only in place for fewer than 4 in 10 small businesses on average.	**Moderate concern about cyber threats** This segment is increasingly alert to cyber threats with 75% a bit or somewhat concerned about the risk of a cyber attack impacting their business.
Less than half are training staff to spot threats While 7 in 10 (67%) think everyone plays a role in cyber security and not just IT experts, only 4 in 10 (40%) businesses are training staff to protect the business from cyber threats.	**Talking about cyber security often** The majority (64%) are discussing cyber security at least monthly. *Discussion of cyber security at least once a year is a requirement for being in this segment. Those who can't recall discussing it were excluded.
Some confidence in preparedness More than 5 in 10 have medium or complete confidence in their ability to prepare for (58%), fight (53%) and recover from (54%) a cyber incident. They are most confident in knowing where to get help when a cyber incident occurs (69%).	**Cyber security still feels overwhelming** 5 in 10 in this segment (50%) still feel overwhelmed when they think about trying to make their business more cyber-safe. Many in this segment view cyber security as too complicated (52%) and too time-consuming (44%) for most small businesses to manage.

Making it easier for the Aware & Emergent to continue their cyber-safe journey

The key objectives for the Aware & Emergent segment are to:

- drive program enrolments
- help simplify small business cyber security to make it achievable.

5.4. Attentive & Maturing

Small businesses in the Attentive & Maturing segment are further along in their cyber security journey but there is room to make their approach more consistent and sophisticated.

Small businesses in this segment think cyber safety is very important. This segment has many cyber-safe practices in place (though they are not as advanced as the most mature segment) and they feel confident in their ability to respond to and recover from cyber threats.

Characterised by their attentive approach, these businesses are well-informed and are very concerned about the risk of a cyber attack. Though many small businesses in this segment are thinking and talking about cyber security regularly, they are still maturing and need to advance their cyber-safe practices and cultivate a consistent culture of cyber safety before they reach the level of Ready & Resilient.

Overrepresented cohorts in this segment include full-time workers, businesses with a physical office, businesses that communicate virtually and businesses that are set up to sell products/services online. Owners/CEOs and employees in this segment were slightly more likely to have an IT or tech background (31% have studied or worked in IT and/or the tech industry).

Attentive & Maturing	
%	12% of sample
Estimated #	
Sole Traders	180K
Micro Businesses	90K
Smalll Businesses	30K

Maturity Index	Medium
Cyber threat perception	**Thinking and talking** about cyber security regularly
Confidence	**High confidence** in their ability to prepare for and respond to cyber threats
Awareness	**Very high awareness** of cyber threats and knowledge about how to be cyber safe
Cyber-safe practices	**Many** cyber-safe practices in place
Cyber-safe culture	**Stronger and developing culture** of cyber safety
Training	**More likely** to be providing cyber security training
Bad habits	**'Bad habits'** are less than average

Cyber skillset	Cyber mindset
Embracing advanced practices Much more likely to have basic cyber-safe practices in place, especially multi-factor authentication on accounts - financial (85%), cloud and social media (75%) and email (70%). On average, advanced cyber-safe practices are in place in more than 6 in 10 businesses.	**Risk-aware and regularly discussing** 6 in 10 are somewhat or very concerned about the risk of cyber attack (62%) the majority are discussing cyber security regularly (36% at least monthly, 24% at least weekly).
Somewhat confident in preparedness Most have medium or complete confidence in their ability to prepare for (73%), fight (62%) and recover from (69%) cyber incidents. 8 in 10 (79%) are confident they would know where to get help. Overall, they are much less likely to have complete confidence compared to Ready & Resilient.	**Cyber security involves everyone** Much more likely to believe it makes a difference when individuals practice cyber-safe habits (85% agree) and see cyber security as everyone's business, not just IT's (90%).
Cyber security training for team members 6 in 10 (62%) report staff receive training about cyber security and how to protect the business from cyber threats.	**Still find cyber security daunting** 5 in 10 (50%) still feel overwhelmed thinking about trying to make their business more cyber secure and 4 in 10 (40%) believe cyber security is too complicated for most small businesses to set up and maintain.

Encouraging the Attentive & Maturing to advance and practice cyber safety consistently

The key objectives for the Attentive & Maturing segment are to:

- reinforce good cyber security progress by embedding Cyber Wardens to support technical uplift with cultural change
- amplify conversation.

5.5. Ready & Resilient

Small businesses in the Ready & Resilient segment have a sophisticated culture of cyber safety. They are thinking and talking regularly about the risk cyber security threats pose to their business and see cyber safety as everyone's business.

These small businesses embed cyber safety in their decision-making and day-to-day operations. Despite their preparedness, they remain pragmatic and do not see themselves as immune to cyber threats.

Small businesses in this segment are prioritising cyber security and are **ready** to respond to threats. Their **resilience** is informed by their characteristic cyber-safe mindset and the myriad foundational and advanced cyber safe practices they have in place.

Certain small business cohorts are overrepresented in this segment, including owners/CEOs, full-time workers, scale-up or start-up businesses, businesses with a physical space, businesses who sell products/services online, and businesses with between 5–19 employees. Small business owner/CEOS and employees in this segment are also much more likely to have an IT/tech background (50% have studied or worked in IT and/or the tech industry).

Ready & Resilient	
%	12% of sample
Estimated #	
Sole Traders	110K
Micro Businesses	100K
Smalll Businesses	40K

Maturity Index	**Most** mature
Cyber threat perception	**Thinking and talking** about cyber security regularly
Confidence	**Very high confidence** in their ability to prepare for and respond to cyber threats
Awareness	**Very high awareness** of cyber threats and sophisticated understanding of mitigation strategies
Cyber-safe practices	**Significant number** of cyber-safe practices in place
Cyber-safe culture	**Sophisticated culture** of cyber safety
Training	**Most likely** to be providing cyber security training
Bad habits	**'Bad habits'** are less than average

Cyber skillset	Cyber mindset
Advanced cyber safe practices On average, 8 in 10 in this segment have advanced cyber-safe practices in place, including limiting apps and software on company devices, deleting and uninstalling old software, and having IT experts configure devices for security.	**Cyber security is front of mind** More than 6 in 10 are talking about cyber security regularly - 30% at least weekly, 34% at least monthly.
Very confident in preparedness More than 8 in 10 have medium or complete confidence in their ability to prepare for (88%), fight (83%) and recover from (82%) cyber incidents. 9 in 10 (91%) are confident they would know where to get help.	**Alert and concerned about cyber threats** 7 in 10 (69%) Ready & Resilient are somewhat or very concerned about the risk of a cyber attack impacting their small business. They are the most likely segment to be very concerned (37%).
Teams trained to identify cyber threats More than 8 in 10 (86%) are training staff to protect the business from cyber threats.	**Cyber security is everyone's business** Most (83%) see cyber security as something everyone plays a role in, not just IT experts.

The Ready & Resilient can be role models for less cyber-safe small businesses

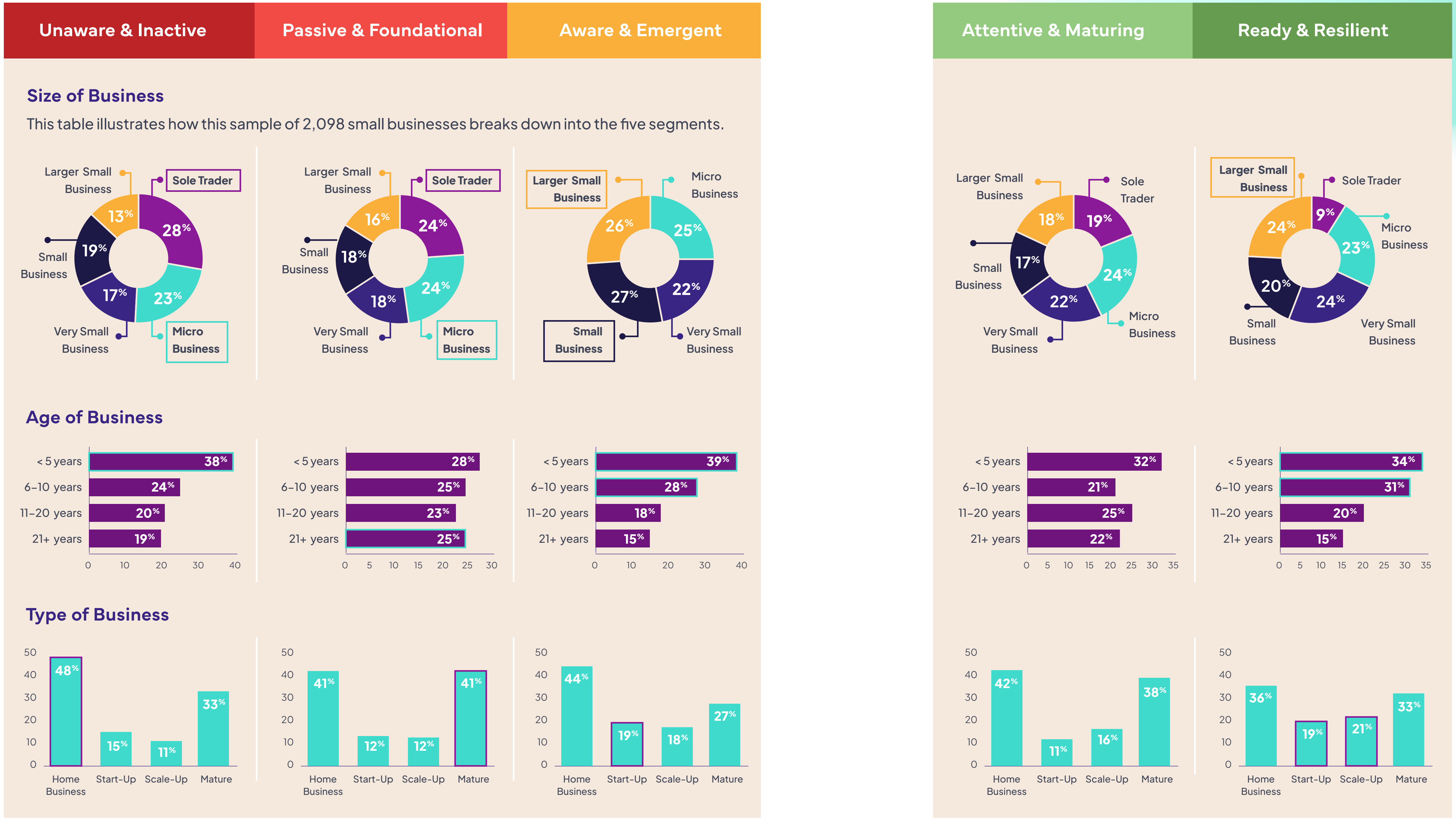
The key objective for the Ready & Resilient segment is to:

- use this segment as a case study and role model for less mature tiers.

5.6. Business size has low influence on cyber safety

The level of a small business's cyber safety has much more to do with its mindset and day-to-day practices than how many employees it has, the age of the business or the type of business. Sole traders, micro-businesses and small businesses with 5-19 employees are represented across all of the small business cyber security segments.

Business Profiles by Segment



6. Barriers to action

Even when small businesses see the value in embracing a culture of cyber security, they face several barriers. They don't know where to begin with cyber security. They feel intimidated by technical jargon, overwhelmed by not knowing what steps to take, and doubtful that they have the time, resources and digital literacy to protect their businesses against cyber threats.

Too much for a small business

More than a third of small businesses (35%) find cyber security practices too time-consuming to implement alongside their existing workload. Small businesses are under pressure and cyber security can fall by the wayside if it's not seen as an integral part of everyday business.

> "I think as a small business we have so many plates spinning and so many other things that are a lot louder and more in your face to tackle than cyber security. Personally, it always just falls by the wayside. If it's not screaming, then it just gets put on tomorrow's to-do list. It's not until something happens that it becomes a higher priority."
>
> Small business (5–19) owner — hospitality (woman, 31, metro QLD)

Overwhelmed and searching for a starting point

Many small businesses don't know where to start when it comes to cyber safety, which can reinforce the unhelpful belief that cyber security is too much for a small business to manage on top of everything else. They are wary of the 'time cost' of getting up to speed and investing in products that are over-promised and under-delivered, given their lack of expertise.

> "I definitely feel like I wouldn't know where to start. I don't have clear steps in my mind. If I knew 'Okay, do this one task today, that will help' at least I've started. I don't even have an idea of where to start, it's not something I see that I can slot in, whereas if I had a 10-step thing, I'd probably do it in bite-size amounts."
>
> Micro business office manager — CCTV and security installations (woman, 34, regional NSW)

Cyber security isn't for 'people like me'

Small business teams are primed to disengage from cyber security when they encounter technical language and industry jargon because of their low cyber literacy. While 7 in 10 (71%) small businesses agree that we all play a role in cyber security, not just IT experts, many lack the confidence to take steps to become more cyber-safe. More than 4 in 10 (43%) small businesses believe cyber security is too complicated for most small businesses to set up and maintain.

> "Most of my team have got very very basic cyber skills. I've explained to the staff why I want to change what we're doing [to become more cyber secure]. I get whining and grumbling about it but in a week or two it will pass."
>
> Small business (5–19) general manager — Aboriginal corporation (man, 50, regional NT)

> "I would, in all honesty, call my best friend's husband who works in IT. Cyber security isn't his field, but that would be who I'd call because he's the only person that I know who will have any idea."
>
> Small business (5–19) owner — hospitality (woman, 31, metro QLD)

A constantly changing threat landscape

The rapidly evolving cyber security landscape poses an additional challenge to small businesses.

Small businesses at various stages of their cyber security journey have some awareness that threats and technologies are constantly developing — though awareness is greater in small businesses that are already prioritising cyber safety. This provokes concern that cyber-safe practices and awareness of cyber threats can quickly become outdated.

> "Being a small business we are always a target and no matter how much protection you have, hackers are always one step ahead."
>
> Small business (5–19) owner - wholesale fashion (man, 38, metro VIC)

7. Driving change

7.1. There is an appetite to upskill and trust benefits to be gained

Small businesses are open to learning simple, practical ways to make their businesses more cyber-safe. Almost nine in ten (86%) expressed a keen interest in a program that simplifies cyber security and makes it achievable for businesses of all sizes.

Most see the value in having team members trained to identify, respond to, and get help with cyber threats. Enhanced cyber security not only safeguards the business but also enhances job security, fosters better client relationships, and instils peace of mind among stakeholders. The majority (68%) believe that prioritising cyber safety builds trust and confidence and shows that a small business cares about their employees, customers and clients.

There is a clear link between thinking and talking regularly about cyber security and having more cyber-safe practices in place and a more established culture of cyber safety. The most cyber-safe small businesses are also the most confident in their ability to respond to and recover from cyber threats.

7.2. The six steps to addressing common barriers

There are significant opportunities to increase understanding of small business cyber threats and build urgency to develop cyber-safe practices and culture competencies by addressing common barriers to small business cyber safety.

1. Tell relatable cyber security stories about small businesses

Many small businesses don't see themselves as being at risk and this stands in the way of them taking steps to protect themselves. Being in the dark about the risk of cyber threats is keeping small businesses vulnerable. A major reason for small businesses to underestimate their vulnerability is that they don't hear about small businesses getting attacked.

Building awareness and urgency starts with telling stories about relatable and local small businesses being attacked and about small businesses benefiting from taking steps to be more cyber-safe.

2. Get small businesses thinking and talking about cyber security

The most cyber-safe small businesses have a cyber-safe mindset and are intentional in their approach to cyber security. Thinking and talking about cyber security is the first step toward building a culture of cyber safety in a small business but many small businesses are not discussing cyber security regularly, or at all.

Conversations are critical to building awareness of cyber threats, encouraging cyber-safe practices and cultivating a cyber-safe mindset in a small business.

3. Encourage cross-pollination of cyber-safe workplaces and people

Exposure to people and workplaces who prioritise cyber safety has a big impact. With every small business that cultivates a culture of cyber safety, there will be a knock-on effect where owners/CEOs and employees will spread this mindset to people in their networks and future workplaces.

Time spent in environments where cyber security is prioritised, and around people who act in a cyber-safe manner, normalises a cyber-safe mindset with a trickle-down effect on other small businesses.

4. Make cyber security something everyone can be part of

A major barrier to cyber safety is an entrenched view of cyber security as something technical that is best left to experts. The use of technical language and industry jargon often deters small business people and cements unhelpful ideas of cyber security as something out of reach for those who are not 'IT-savvy'.

Embracing accessible language sends the message that cyber security is for everyone. This makes it easier for small business owners/CEOs and employees to talk about cyber security and put cyber-safe measures in place no matter their level of technical know-how.

5. Break cyber security into bite-sized pieces/make it achievable

Time and resource-poor small businesses caught up in day-to-day operations are not thinking much about cyber security. When they do, they often feel overwhelmed and don't know where to begin, often assuming cyber security will require considerable time, money and energy to address.

By breaking cyber security down into bite-sized pieces, small businesses will have access to easy, practical steps they can take to help protect themselves. Simplifying the way we address cyber security is key to taking it out of the 'too hard basket' and making it achievable and actionable for every small business.

6. Frame cyber security as a two-way street

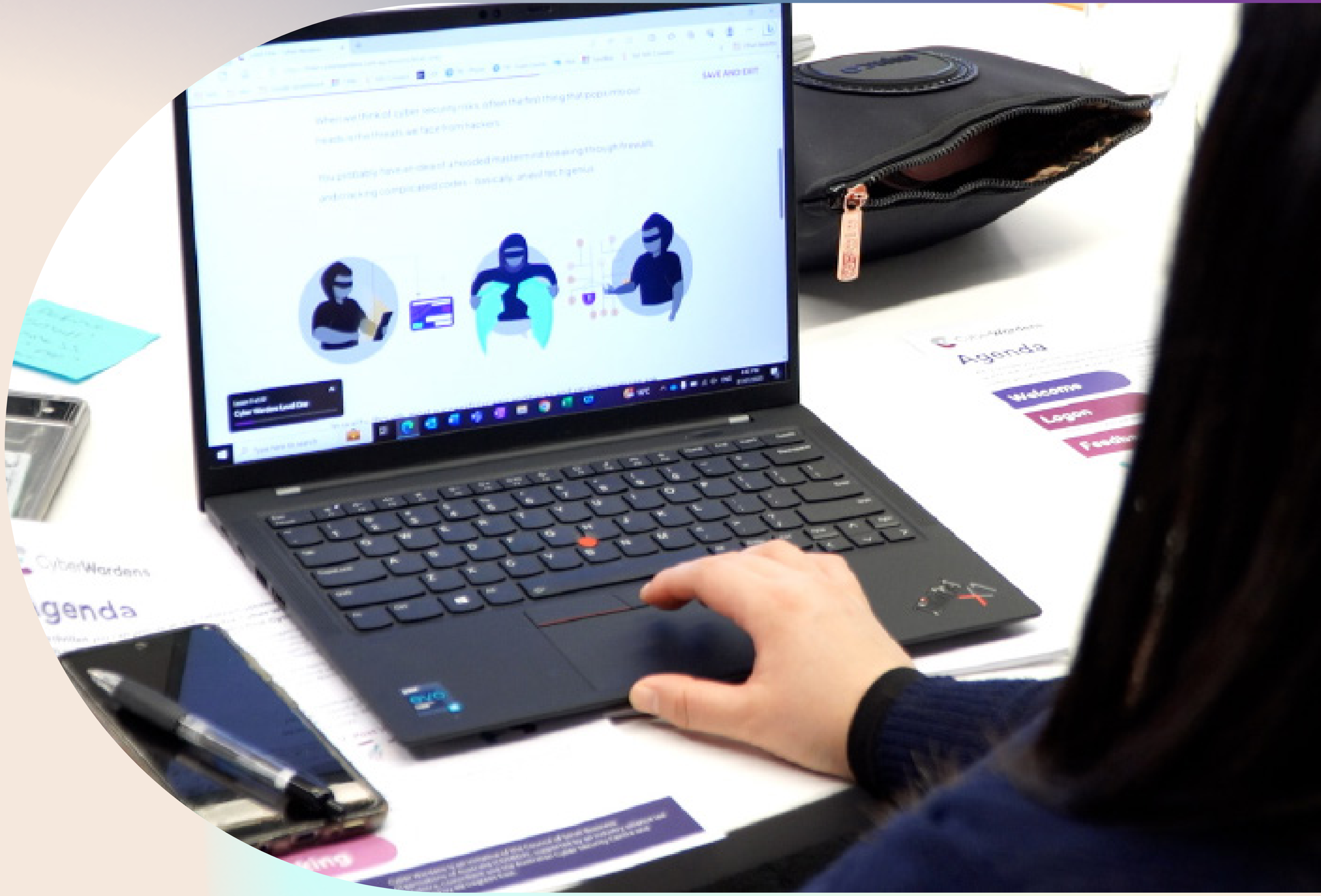
Small businesses rely heavily on the security of platforms they use every day and the trust they place in third-party providers. Their confidence that these providers are too big to fail, coupled with not knowing what steps they could be taking themselves, means many small businesses are not putting important protections in place on their end.

Communicating that third parties are partners, rather than protectors, of small businesses, is key to encouraging small businesses to work with third parties and take steps to help protect themselves.

CyberWardens.

Small business cyber security simplified.

Help your business to be cyber-safe with free Cyber Wardens training.



Learn more at cyberwardens.com.au

Cyber Wardens is an initiative of the Council of Small Business Organisations of Australia (COSBOA), supported by the Australian Government and an industry alliance led by Telstra, CommBank and the Australian Cyber Security Centre.

CyberWardens.

Proudly
supported by

Australian Government

COSBOA