CyberWardens.

2023–2030 Australian Cyber Security Strategy

Submission on behalf of Cyber Wardens

Executive Summary

1. Small businesses are time-poor and need fit-for-purpose solutions with simple language and a small number of basic, small steps to make incremental improvements.
2. The CyberWardens programme uplifts small businesses by educating an in-house "Cyber Champion" similar to a Workplace Safety Officer building cultural competencies alongside technical know-how.
3. Given the resource challenges of small businesses, Cyber Wardens endorses the Government stated goal to shift the systems burden of cyber security to those best able to do so but strongly advocates the need for urgent small business education and awareness support to meet the increased risk of cyber-attacks whilst system changes take effect.

1. Introduction

As specialists in small business cyber security education, Cyber Wardens enthusiastically acknowledge the government's ambition for Australia to be a cyber-security superpower by 2030.

Australia's entrepreneurial heart is comprised of 2.3 million small businesses. Small business is our largest employer, taking on 5 million people and contributing $418 billion to Australia's GDP.

The government has rightly recognised the need to support Australian businesses, particularly small businesses, in meeting the cyber challenge.

Proudly supported by

COSBOA COUNCIL OF SMALL BUSINESS ORGANISATIONS AUSTRALIA

89 DEGREES EAST DATA STRATEGY DELIVERY

1.1. Unique cybersecurity threat to small business

While the online ecosystem presents a myriad of opportunities for small businesses to innovate and economise, it also elevates the risk of a cyber attack. Small businesses are increasingly cognizant of the risk that cyber threats pose to their business, their financial security, privacy and livelihoods. Recent high-profile breaches of major corporations have heightened concerns and reinforced the vulnerability faced by small businesses.

For many small businesses, the boardroom and the family dining table are one and the same, increasing the vulnerability. While they are experts in their own businesses, they lack time, resources, expertise and energy to manage a problem they are not familiar with.

Small business see cyber security as an expensive technical problem, misjudging the threat as purely technical rather than capability driven. Owners believe they lack IT skills and resources to solve the problem and underestimate their relative vulnerability as too small to matter.

Given 19 out of 20 successful cyber attacks target people, meeting the challenge of small business cyber security means investing in the cyber-safe mindset and capabilities across the small business landscape.

1.2. Cyber Wardens mission

Cyber Wardens is a world-first initiative of the Council of Small Business Organisations of Australia (COSBOA), supported by an industry alliance led by Telstra and CommBank and delivered by 89 Degrees East to build a cyber-safe workforce protecting small businesses from online threats.

Our aspiration for Australian small businesses to operate in a cyber-safe environment strongly aligns with the Government's aspiration for Australia to be a cyber security superpower over the coming decade.

By bolstering the cyber capabilities of people who work in small business, we make it easier for small business to increase their cyber posture, which prevents attacks and builds resilience to them when they occur. As an example, more than 70% of rural and regional small businesses do not have an outsourced tech provider - which means it is critically imperative we help them build in-house skills.

As Australia's peak body for small businesses, COSBOA has a proud history of strong advocacy on small business issues ranging from taxation and workplace relations to competition law and retail tenancy.

For the past 18 months, COSBOA has been responding to the concerns of small businesses around the country by working in partnership with 89 Degrees East o develop this innovative pilot. Cyber Wardens is based on significant consumer research to ensure the program is a purpose-built solution.

1.3. Lessons from workplace safety

Leveraging COSBOA's grassroots infrastructure and reputation to change behaviours, Cyber Wardens will be the online version of first aid officers or fire safety wardens. Cyber Wardens will be equipped to prevent, prepare, fight and help recover from a cyber attack or the theft of customer data or intellectual property.

Just like Work Health and Safety officers help keep small business safe from physical hazards, Cyber Wardens use the same skills to prevent and protect against digital threats.

The model draws strong parallels to Australia's experience building physically safe work environments. Major reforms to improve workplace safety have been championed and adopted by workplace safety officers. To meet the workplace safety challenges of this century, Cyber Wardens will establish a frontline of cyber security champions capable of spotting hazards, reducing risks, and providing the equivalent of cyber first aid.

Cyber Wardens will complement Australia's growing pool of cyber technical experts to drive cultural change and cyber-safe mindsets in Australia's small business.

Having a trained Cyber Warden who can identify and prevent a single attack would save a small business $50,000 on average.

Whilst the need is greatest in resource-poor small businesses, the role of a Cyber Warden would benefit companies and organisations of all sizes.

1.4. Behavioural change requires whole sector action

Resource-poor, small businesses cannot go it alone. Small business face a supply chain lockout that will detrimentally impact both small and large businesses alike unless they are supported to build their cyber capabilities.

Cyber Wardens is backed by an alliance of Industry and Government supporters who are committed to helping small business build their cyber-safe capabilities. Cyber Wardens is seeking to further work with the Government to extend the pilot and create a pathway for small business cyber skills development.

Only together can we impact sector-wide change and protect the small business supply change.

1.5. Urgent small business assistance required

Cyber threats are becoming more frequent, sophisticated, and costly for Australian businesses. Cyber insurance can help businesses and individuals mitigate the financial impact of cyber-attacks and data breaches. However, premiums in Australia range from $1,500 to $60,000 per year for small to medium-sized businesses and are often hard to access.

Given the resource challenges of small business, Cyber Wardens endorses the Government stated goal to shift the systems burden of cyber security to those best able to do so. In the long term, this will provide meaningful change and make the operating environment safer for both small business and customers alike.

Initiatives that champion security by design, such as decoupling user logins from active seat licencing in pricing models, would enable better implementation of small business cyber security practices. These systems reforms will take time to impact and benefit small businesses, while the threat faced by small business is urgent.

Our research shows that 44% of small businesses have faced an online security threat, and that number will only increase.

By acting to expand the Cyber Wardens program, the Government can rapidly scale a purpose-built solution, ensuring the urgent role of support and skills development to complement system change.

1.6. About this submission

The following submission specifically responds to six of the consultation questions.

Given our experience and perspective is anchored in small business, we start by comprehensively responding to consultation Question 15, focussing on how government and industry can work together to improve best practice knowledge and behaviours in small businesses.

Cyber Wardens could also partner with the government to extend its reach into some of the other areas outlined in the consultation paper. Cyber Wardens could help facilitate best practice and information sharing (consultation questions 6 and 7) as well as help upskill and support Australia's workforce (consultation questions 11 and 12). Once established and with the right support, Cyber Wardens is well placed to help the government address these challenges in the small business community. We have also outlined some other ideas in response to these questions, along with how to address emerging technologies while at the same time promising new security-by-design technologies (consultation question 19).

Our policy recommendation specifically outlines the government support needed to ensure the established Cyber Wardens program can help the small business community manage its cyber security risks, with a particular emphasis on keeping their data, and their customer's data, safe.

Key recommendation:

A government investment of up to $23 million would result in at least 15,000 Cyber Warden Small Businesses, supported by 50,000 trained Cyber Wardens and additional awareness activities supporting more than 1 million small businesses and 6 million Australians.

1.7. Sector-wide endorsement

Cyber Wardens has strong support across the small business landscape as a solution designed to meet the challenges of small business cyber security education.

Matthew Addison, Chair COSBOA

> *"Small Business tell us that they hear about Cyber Security risks but don't know what to do or if they can do anything. They also tell us there is so much information they don't understand. COSBOA supports action-based behaviour change information for small business. COSBOA research and engagement has led to the CyberWardens model to enable education and enhanced security for the people in small business."*

Andrea Moody, Acting CEO, Family Business Australia

> *"Family Business Australia is proud to support the Cyber Wardens Program, we believe this initiative will provide valuable training and resources to help individuals and organisations protect themselves against cyber threats. As family-owned businesses are often targets of these threats, it is crucial to educate our members and the broader community about cybersecurity best practices."*

Amanda Linton CEO Institute of Certified Bookkeepers (ICB)

> *"Bookkeepers face cyber threats themselves and see them in the many businesses they support. ICB support the actions proposed to change the behaviour of small business to assist in their protection against cyber attack and also their recovery following attacks. Small business orientated actions that can be taken one step at a time assisted by their trusted advisors."*

Simon Forster, Immediate Past President of DSPANZ

> *"Time-poor small businesses will benefit fit-for-purpose solutions with simple language and a small number of basic, small steps to make incremental improvements like the Cyber Wardens program."*

Scott Seddon, President, Independent Cinemas Australia

> *"Today's cinema projectors are completely digital and are all operated within secure networks. If this security was breached, the operation of projectors and screen servers could be disrupted or even permanently damaged. In today's world, most cinemas operate loyalty programs, most also offer tickets and, in many cases food sales online. Independent Cinemas Australia is looking forward with enthusiasm to the rollout of the Cyber Wardens Initiative as it has the potential to allow members to actively protect themselves from the countless cyber security threats to businesses everywhere, every day."*

Sandy Chong, CEO Australian Hairdressing Council

> *"AHC will be supporting and promoting Cyber Wardens role out, engagement and uptake to our members. We have ongoing concerns regarding cybercrime and want our industry to be well-informed and educated on best practice.*
>
> *We can all be a target, AHC wants to ensure that every small business is prepared with the right information from a trusted source."*

2. Small Business Cyber Security

2.1. Consultation question 15: Government and industry working together to improve cyber security best practice knowledge and behaviours.

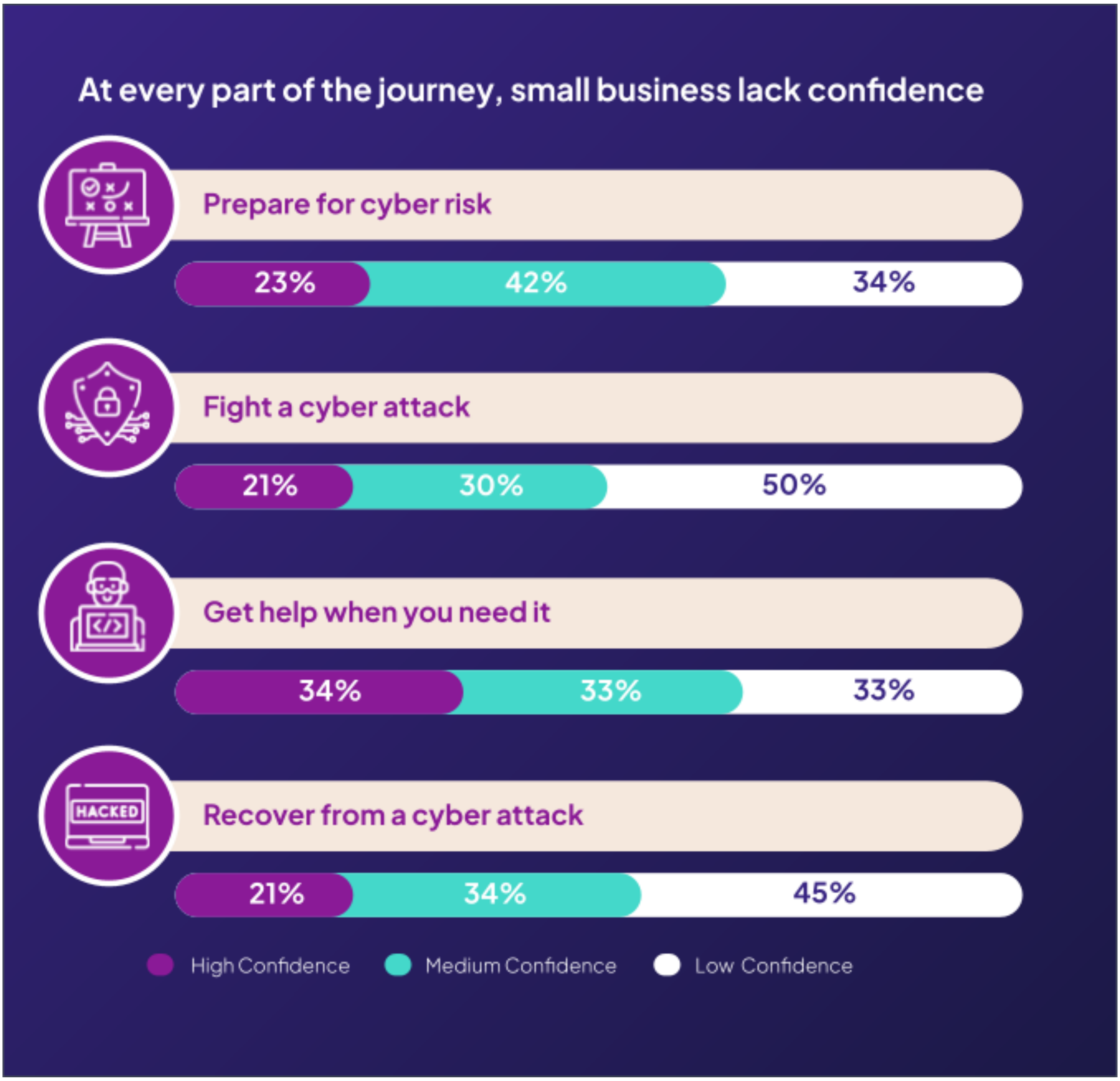
Small businesses see cyber security as an expensive technical problem, they underestimate their relative vulnerability and believe they lack the IT skills and resources to solve the problem. Small business recognised a 13% increase in cyber attacks during 2021. 43% of cybercrime targets small businesses, and while 6 out of 10 small businesses are at serious cyber risk, they are not confident in their practices.

2.1.1. Research findings from the small business community

Between November and December 2022, 89 Degrees East conducted quantitative and qualitative research activities, including a survey of more than 2,000 Australian business owners (564) and employees (1,553) as well as focus groups with 18 small business owners (including 8 sole traders).

The research found that **cyber is a critical concern,** ranking second in order (37%) to energy prices (41%) and before interest rates and access to finance (34%). 36% of all participants stated they had a high or very high concern about the risk of a cyber security attack.

Unfortunately, this level of concern is not currently matched by confidence, knowledge and preparedness. At every part of the journey - be it preparing for cyber risk, fighting an attack, getting help, and recovering - small business owners know they are **underprepared.** Only 21% of business owners and employees feel confident that they know how to fight a cyber risk and how to recover from a cyber attack.



The research quantified what we already knew anecdotally - **that cyber attacks are becoming all too common in the small business community.** 44% of participants had experienced a cyber attack of some nature, with a close-to-even split between a personal cyber attack (29%) and business-related cyber attack (22%).

44%
Have experienced
A cyber attack

29%
Personal
Cyber attack

22%
Business
Cyber attack

Views toward risks and concerns relating to cyber attacks amplify significantly after an individual has had their cyber security compromised. Whether that incident is personal or professional in nature, it triggers a heightened interest and concern in cyber security. Unfortunately, this happens once it is too late - an attack has occurred, data has been compromised, and any time that could have been spent on prevention is quickly chewed up by recovery.

The findings on small business cyber posture are perhaps more alarming than we could have anticipated. While we know that **small businesses struggle to implement a proactive cyber posture**, we did not appreciate that half would have basic password vulnerabilities (only 53% have consistently turned on MFA), and only half have a basic practice of not sharing passwords (54% consistently do not share passwords). Most small businesses struggle to identify specific cyber security attacks, and only a third demonstrate behaviours consistent with all of the Essential 8 cyber security behaviours.

The overwhelming majority (81%) of participants are ready to take responsibility and understand that cyber security is a challenge for all of us, not just something to be left to IT experts. A similarly overwhelming majority of business owners and employees (85%) agree that it's important for business owners to encourage a culture of cyber safety. Importantly, these results were consistent amongst business owners and employees.

Small businesses are most concerned about a cyber attack resulting in a loss of customer data or personal information, hackers accessing company bank accounts and loss of company data such as financial information and intellectual property. Businesses operating in the health care, caring and support services sector over profile for being most concerned about the loss of customer data or personal information (50% rated first concern). It is also worth noting that, for several participants, the idea that they had private client data which could be hacked only dawned on them as the focus group discussion unfolded because they had not previously turned their minds to this issue.

Small businesses are increasingly aware that cyber safety needs to be a cultural skill for the whole business. Yet almost 1 in 2 small business owners and employees view cyber as too hard, prohibitive and too complicated to maintain. There is also a common misconception that SAAS software would protect them.

Research Data

The ***'Understanding Small Business & Cyber Security Report'*** was undertaken by 89 Degrees East and conducted between November and December 2022.
The findings are drawn from quantitative and qualitative research activities, including:

- a survey of more than 2,000 Australian business owners and employees. The sample included views from 564 Australian business owners and 1,553 Australian employees.
- focus groups with 18 small business owners, including 8 sole traders.

A copy of the raw data is attached to this submission.

Fit-for-purpose solutions

It is not surprising that 4 in 5 small business owners and employers believe the Cyber Wardens initiative will support them. This is especially true of employees and female founders.

There is an overwhelming view amongst small businesses that quick incremental wins are essential for this time-poor group. Perfect is the enemy of good for time-poor small business owners.

Prioritising small steps can make a big difference, and the Commonwealth Government has a responsibility - and opportunity - to help small business owners get the vital basics right.

Too much detail will paralyse small business owners. It is essential that education initiatives are accessible and scaffold learning using non-technical language.

Small businesses can see that the Cyber Wardens program helps them protect money, emails and data, which protects their overarching ability to operate. Some saw a secondary benefit in being able to promote themselves as a Cyber Safe business.

The most favourable attributes of the Cyber Wardens program were:

- No cost, it's free (53%)
- Making cyber security easier for small business (49%)
- Helping to train team members to spot and stop cyber attacks (42%)
- Providing mobile learning, fast and in your pocket, when you have five minutes (36%)
- Tailoring the solution as one that is made for small business, by small business (36%)

The first two attributes listed above were even more favourable to female founders, with 71% noting no cost and 63% noting that the program makes cyber security easier for small businesses.

Most participants wanted to learn the basics quickly, but with the option of several tiers to go deeper. The preferred approach was one hour per week over four weeks, with an opportunity to further update once a year, given cybercrime is an evolving challenge. Small businesses with employees noted that a shorter course of 45 minutes could be useful in monthly team meetings or even social events when employee participation could be incentivised.

2.2. Consultation Question 15a: Government equipping and enabling small businesses to manage their cyber security risks to keep their data and their customer's data safe.

The Cyber Wardens infrastructure is built and ready to roll out, but government support is required to scale this effort to one that has the capacity and reach to establish a Cyber Wardens Frontline in small businesses across the country.

This is important for small businesses and their customers, but also their broader supply chains. A cyber attack on any part of the supply chain can have a ripple effect that can disrupt operations and cause financial and reputational damage.

A cyber attack on a supplier or vendor can disrupt the operations of the entire supply chain, causing delays in the production and delivery of goods and services, exposing the exchange of sensitive information, resulting in significant financial loss and reputational damage.

Clearly, support for a cyber-secure small business community has broader benefits across the economy.

Cyber reforms must enable small businesses to thrive. This is not about burying them in a weighty unaffordable process. Instead, reforms should simplify processes, provide guidance and support and make it easier for them to implement robust cybersecurity measures.

A three-year investment from the Australian government would deliver Australia's first small business cyber security frontline, made up of employees and owners from the nation's 2.3 million small businesses. This investment would supercharge behavioural change in homes and businesses across Australia - with heightened knowledge and safer online practices embedded in the small business community culture.

Government support for this initiative would help roll out the program across the country. As demonstrated below, the program can be scaled. The greater the government funding injection, the greater reach the program will achieve in that three-year period. A $23 million government investment would result in at least 15,000 Cyber Warden Small Businesses, supported by 50,000 trained Cyber Wardens and additional awareness activities supporting more than 1 million small businesses and 6 million Australians.

Policy recommendation:

$15 million government + Industry Investment	**$23 million** government + Industry Investment
Cyber Wardens Scaled eLearning Program + Resources Hub	
National government and Industry Alliance and sponsorship	
5,000+ Cyber Warden Small Businesses	**15,000+** Cyber Warden Small Businesses
20,000+ trained Cyber Wardens	**50,000+** trained Cyber Wardens
Behavioural change 400,000+ small businesses more cyber aware 3 million Australians more cyber aware National Roadshow, including 12 events	**Behavioural change** 1 million+ small businesses more cyber aware 6 million Australians more cyber aware National Roadshow, including 24 events

The Cyber Wardens program can also support the government as an information conduit to the small business community. For example, Cyber Wardens could play an integral role in supporting the activities wrapped up in consultation questions six and seven. With the right support and arrangements in place, Cyber Wardens could support the government by using best practice examples in its eLearning modules and by alerting the network to cyber threats.

2.3. Consultation question 6: Commonwealth government leading by example.

The government needs to clearly, consistently and publicly communicate that a security-first approach should always be adopted, with security integrated into all aspects of the department or agency's operations.

Public communications should demonstrate that the government is leading the way, setting a benchmark that individuals and industries must follow.

Departments and agencies should share threat intelligence with other entities in the public and private sectors to help build a stronger cybersecurity ecosystem.

COSBOA's extensive experience in awareness and community engagement campaigns with small businesses consistently demonstrates that awareness and education campaigns must be grassroots and peer-led if they are to have a meaningful impact on small business owners.

As noted above, Cyber Wardens could be a conduit for information sharing within the small business community.

The Australian government can require accreditation for those working in cyber security in sensitive industries. This can help ensure that cybersecurity professionals have the necessary skills and qualifications to do their job effectively. It can also collaborate with other governments and international organisations to develop global standards for cybersecurity education, immigration, and accreditation.

2.4. Consultation question 7: Improve information sharing with industry on cyber threats.

The Cyber Wardens program could certainly help share relevant information through its extensive networks, but it is important to note that awareness campaigns must be specifically directed at small business and be tied to practical initiatives.

Cyber threats are continually evolving, and small businesses may not be aware of the latest threats and trends. Targeted awareness programs can help small businesses stay up to date with the latest cybersecurity threats and how to mitigate them.

Tying cybersecurity awareness programs for small businesses to practical outcomes provides actionable insights, helps allocate resources effectively, demonstrates measurable results, mitigates risk, and outlines the return on investment. By focussing on practical outcomes, small businesses can better understand why they need to protect themselves against cyber threats and thrive in a digital age.

The Australian government could develop a comprehensive framework for information sharing on cyber threats. This framework should provide guidelines for sharing information, define the scope of information to be shared, and establish clear procedures for handling and safeguarding sensitive information. Cyber Wardens could form part of the information thread for this work.

The government could also offer incentives to encourage industry to share information on cyber threats. For example, it could provide financial incentives, legal protection, or other benefits to companies that participate in information-sharing initiatives.

The government could foster a culture of trust between government agencies and industry by establishing clear lines of communication, building relationships, and demonstrating a commitment to transparency and collaboration.

The government also has a key role in providing resources that help industry better understand cyber threats and how to protect against them, as well as the importance of reporting threats in a timely manner.

The foundations of the Cyber Wardens infrastructure and eLearning also present an opportunity to customise the core content into other critical sectors, including the not-for-profit sector, community clubs and education.

2.5. Consultation questions 11 and 12: Supporting Australia’s cyber security workforce and uplifting cyber skills beyond the broader STEM agenda.

Democratising cyber security in Australia requires related training that is accessible and understandable to everyday people, regardless of their technical background or expertise.

Australia needs a tailored approach to improving cyber skills beyond the government's broader STEM (Science, Technology, Engineering, and Mathematics) agenda. While STEM education is important for developing a strong foundation in technical skills, existing programs often fail to provide the specific knowledge and training needed for a career in cyber security.

It is also important to emphasise that **training and access must be available to people outside formal education**, because we all must operate as cyber secure individuals.

While large employers are already investing in cyber-skill awareness education for their employees, small business employees do not have the same level of access.

The Cyber Wardens program democratises cyber learning by applying it across the small business workforce in a way that is applicable and implementable in a workplace setting but also relevant to personal circumstances. It does not require prior training or knowledge and places a premium on practical work skills.

The Cyber Wardens program has the potential to provide a pipeline of skilled students who are ready to develop their technical skills and join Australia's cybersecurity workforce on a larger scale. It is very possible that Cyber Wardens provide small business employees an introduction to the opportunities of a cyber career that they would not have otherwise known existed; this could be particularly profound amongst young employees.

Boosting the general cyber literacy of small business owners and employers will drive cultural change and develop cyber-safe mindsets in Australia’s small business community. Our research shows that the small business community urgently needs the Cyber Wardens pathway to this positive transformation.

2.6. Consultation question 19: An evolving strategy that is agile to new and emerging technologies.

The legacy benefits of the Government's investment in scaling the Cyber Wardens program will apply to both the program and the people.

In our research with small business owners, it was immediately apparent that the cyber threat would evolve and that Cyber Wardens would need annual refreshers to respond to emerging threats, much like first aid officers do.

Government investment would facilitate the development of an annual Cyber Wardens recertification program designed to keep the program and its training up to date in a rapidly evolving cyber risk context. This would allow for up-to-date messaging, as well as information and best practice sharing.

Further, the Cyber Wardens digital infrastructure will support mini modules on industry-specific and emerging technologies, which will facilitate deeper dive and extended learning.

The national network of Cyber Wardens will be regularly supported with ongoing communications to ensure they are well-informed on emerging technologies.

3. Conclusion

Small business is the powerhouse of Australia's economy, making up about 98% of all businesses and accounting for around 35% of the country's GDP. Small businesses are major employers in Australia, providing jobs for almost half of the country's workforce. This creates employment opportunities for Australians and contributes to the overall growth and development of our country.

The small business sector is ready to step up to the challenge of reducing its cyber risk. It sees cyber security as a whole-of-society and whole-of-business responsibility and understands its people are best placed to manage the elevated risk in their businesses and their sectors.

The Cyber Wardens program provides a low-cost, user-friendly approach to equipping the small business community in a way that does not unnecessarily or unfairly burden them.

The Cyber Warden program enables them to take responsibility and, with that, take control.

The Cyber Wardens program is established and ready to go. Through our research, we know that it meets the needs and expectations of small business but the program requires government financial support if it is to efficiently scale up to meet the urgent need.

A $23 million government investment would result in at least 15,000 Cyber Warden Small Businesses, supported by 50,000 trained Cyber Wardens and additional awareness activities supporting more than 1 million small businesses and 6 million Australians.

Cyber Wardens creates a cyber-frontline across individual businesses, reduces their risk, and saves them money, along with their customers and those in their supply chains. Having a trained Cyber Warden who can identify and prevent a single attack would save a small business $50,000 on average.