COUNCIL OF SMALL BUSINESS ORGANISATIONS AUSTRALIA

Secretariat: PO Box 463
Canberra ACT 2600

0493 364 720

Our advocacy team is based in Canberra

Email: ceo@cosboa.org.au
www.cosboa.org.au

Office of Home Affairs
Via email: auscyberstrategy@homeaffairs.gov.au

14 April 2023

Dear Sir/Madam,

Re: 2023 – 2030 Australian Cyber Security Strategy

Thank you for the opportunity to submit our contribution towards the development of the 2023 – 2030 Australian Cyber Security Strategy.

The Council of Small Business Organisations Australia (COSBOA) appreciates the consultation process and the Government's commitment to bolstering cyber security with a view to making Australia the most cyber secure nation in the World by 2030.

Our vision is for small businesses to be appropriately engaged in a scaled approach to cyber security. We believe that burdensome regulations, requirements, and penalties could lead to disengagement, resulting in a less secure and protected cyber environment.

On behalf of COSBOA, this submission seeks to highlight key consideration for small business as it relates to accessible, affordable, achievable and manageable cyber security measures for the sector. It will provide evidence-based strategy recommendations relevant to COSBOA members and stakeholders generally.

1. Introduction

1.1 Background

This submission aims to contribute in a practical way to the formulation of the 2023 – 2030 Australian Cyber Security Strategy (The Strategy).

The Office of Home Affairs has identified three sets of opportunities to explore through consultation on the Strategy:

1. How Australia can elevate the existing level of engagement with international partners through concrete steps to promote cyber resilience?

2. What opportunities are there to better support the development of international technology standards, particularly in relation to cyber security?

3. How can government and industry partner to uplift cyber resilience and secure access to the digital economy, especially in Southeast Asia and the Pacific?

The digital economy has brought numerous benefits, but it has also led to increased risks, such as data hacking, identity fraud, reputational damage, and blackmail, due to the generation, use, disclosure, and storage of large amounts of personal information.

Trust in technology is vital for fostering economic development. The challenge lies in realising the benefits of data-driven technology while safeguarding the cyber environment– something of global concern.

COSBOA acknowledge that there are many emerging technologies and artificial intelligence that will significantly impact, and be impacted by, cyber security.

Some of these technologies exist now. Others will rapidly develop from 2023 to 2030 and will disrupt the existing landscape of cyber security.

COSBOA believes that the Strategy must be adaptable to account for changes in the strategic and technological environment in the coming years and must be accessible and relevant to Small Business irrespective of their size and available fiscal and human resources.

1.2 Testimonials from our Key Stakeholders

Simon Foster, Chair, Govt & Stakeholder Relations Committee of DSPANZ

"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.

Given the resource challenges of small business, the cyber security systems burden should be shifted to those best able to do so - Federal & State Government, larger enterprises and software providers.

The CyberWardens programme addresses much of this, and uplifts small business cyber posture by educating an inhouse "Cyber Champion" similar to a Workplace Safety Officer."

Andrea Moody, Acting CEO, Family Business Australia

"Family Business Australia is proud to support the CyberWardens 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."

Scott Sneddon – President Independent Cinemas

"Today's cinema projectors are completely digital and are all operated within secure networks. If this security was breeched, the operation of projectors and screen servers could be disrupted or even permanently damaged.

In today's world most cinemas operate loyalty programs and most also offer tickets and in many cases food sales online.

Independent Cinemas Australia is looking forward with enthusiasm to the roll out of the CyberWardens Initiative as it has the potential to allow members to actively protect themselves from the countless cyber security threats to businesses everywhere, every day."

Christine Pope, Director of ATMS

"Small businesses in the healthcare space hold more and more information electronically and value the support of projects such as CyberWardens to inform and educate them about security risks and how to manage those risks in their businesses.

There is so much information in this area and it can often be quite overwhelming so it's important to have the information from a trusted source."

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."

Sandy Chong, CEO Aust Hairdressing Council

"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.

Given the resource challenges of small business, CyberWardens endorses the Government stated goal to shift the systems burden of cyber security to those best able to do so

The CyberWardens programme uplifts small businesses by educating an inhouse "Cyber Champion" similar to a Workplace Safety Officer."

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."

1.3 Goal

As with all our contributions to the cyber safety discussion, COSBOA's submission supports Australian small businesses by advocating for a tailored and targeted educative services approach, investment in cyber security infrastructure, and a balanced and achievable approach to cyber security regulatory requirements.

2. Executive Summary

In preparing this submission COSBOA consulted with a range of stakeholders, including Tech Council of Australia (TCA), Communications and Information Technology Training (CITT), Australian Small Business and Family Enterprise Ombudsman (ASBFEO), CPA Australia, Pharmacy Guild, the Australian Hairdressing Council (AHC), Institute of Certified Bookkeepers (ICB), and DSPANZ.

2.1 Key recommendations

COSBOA's key recommendations for the Strategy are:

1. **Best Practice:** Provision of small business best practice guidelines
2. **A Designated Certification Scheme:** Expansive roll-out of CyberWardens as the designated cyber essentials certification scheme.
3. **Continued Support:** Continued support of small businesses including a limitation of non-compliance penalties.
4. **Leverage Investment in a Scale-able Solution:** Investment in CyberWarden's national roll-out as a certification-based solution will set a new standard for micro market players and will formalise the pivotal role they play in any first or developing world economy.

These recommendations aim to support small businesses while ensuring cyber security and consumer confidence.

3. Issues and Recommendations

3.1 Issue 1: What assistance do small businesses need from government to manage their cyber security risks to keep their data and their customers' data safe?

3.1.1 Background

Compliance with cyber security legislation is an ongoing process., and small businesses must manage various aspects to prevent breaches and ensure adherence.

Information technology presents immense opportunity for small businesses to reach new markets and increase productivity and efficiency.

However, with this opportunity comes increased risk. To mitigate this risk, small businesses need a cybersecurity strategy to protect their own business, their customers, and their data from growing cybersecurity threats.

3.1.2 COSBOA's Position

To reduce small businesses' risk of contravening cyber security laws, legislative reform should be accompanied by government-endorsed best practice guidelines

3.1.3 Evidence

COSBOA's CyberWardens program and associated research – which will be further explained later in this submission - reveals that small businesses lack sufficient knowledge regarding both their cybersecurity obligations and how best to manage data that they secure, store and utilise in business practice.

Fundamental knowledge such as what constitutes data, whether a business holds data, and how and why it is sourced and stored is lacking across all industries.

3.1.4 Recommendation

Provision of small business best practice guidelines

We recommend that any legislative reforms should be accompanied and supported by government-endorsed best practice guidelines and fit for purpose program like CyberWardens to provide practical advice for small business compliance.

To ensure effective communication with small businesses, COSBOA strongly recommends that industry is consulted and engaged in developing these guidelines.

3.2 Issue 2: What opportunities are available for Government to enhance Australia's domestic cyber security technologies ecosystem and support the uptake of cyber security services and technologies in Australia?

3.2.1 Background

Consumers increasingly consider data protection in their choice of digital services, and small businesses often lack the resources to manage their data protection obligations effectively.

3.2.3 Evidence

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, through to competition law and retail tenancy.

Responding to the concerns of small business around the country and as a result of its significant consumer research, COSBOA for the past eighteen (18) months has in partnership with 89 Degrees East, developed an innovative purpose-built solution - the CyberWardens program

Supported by an industry alliance led by Telstra and CommBank, CyberWardens represents a world first cyber-safe workforce initiative that builds small businesses capacity to manage online threats.

By bolstering the cyber capabilities of small businesses, CyberWardens makes it easier for SMEs to bolster cyber protections and to bolster their cyber-attack defences.

3.2.4 Recommendation

The CyberWarden project offers a solution to address the most common internet-based attacks.

COSBOA recommends the expansive roll-out of CyberWarden as the designated cyber essentials certification scheme.

Subscription to the scheme would enable small businesses the capacity to protect the confidentiality, integrity, and availability of data stored on devices that connect to the internet.

The CyberWarden scheme would form a corner stone of the Strategy and would establish a set of baseline technical controls to help SMEs improve their cyber defences and publicly demonstrate their commitment to cybersecurity.

3.3 Issue 3: How should Government seek to monitor the regulatory burden on businesses as a result of legal obligations to cyber security, and are there opportunities to streamline existing regulatory frameworks?

3.3.1 Background

Any proposed increase in non-compliance penalties will disproportionately impact small businesses.

The stark reality is that for the majority of small businesses the combination of a cyber-attack and any associated penalty would effectively push them to insolvency.

3.3.2 Evidence

Recent incidents of data breaches and identity theft, such as those at Optus and Medibank, highlight the need for more robust legislation and defined cyber incident reporting frameworks.

COSBOA's engagement with small businesses show that they are poorly positioned to tackle these reporting requirements, with many remaining confused about what they are expected to do.

3.3.3 Recommendations

COSBOA advocates for support of small businesses as they recover from the Pandemic and associated economic challenges, and to that end, it discourages non-compliance penalisation of any kind.

Adopt a proven model

COSBOA recommends the adoption of CyberWarden which is a fit for purpose solution furnished with resources and training tailored to this sector.

Leverage trusted pathways

In addition to the recommended adoption of CyberWarden, the Strategy should include and leverage trusted pathways such as industry associations and advisors to disseminate information on compliance requirements and support for small businesses.

Continued engagement and consultation

Continued engagement and consultation with industry is crucial.

In developing CyberWarden, COSBOA has engaged with and collaborated with its members, technology and cyber experts and carriers.

In the dynamic cyber security space collaboration is key.

3.4 Issue 4: How can Commonwealth Government departments and agencies better demonstrate and deliver cyber security best practice and serve as a model for other entities?

3.4.1 Background

COSBOA is the national peak body representing the interests of small business.

Collectively, COSBOA's members represent an estimated 1.3 million of the 2.5 million small and family businesses that operate in Australia.

3.4.2 COSBOA's Position

Small business employs 68% of Australia's workforce. In GDP terms, SMEs together contribute 56% of value added.

As it has been evident not just in the preparation of this submission, but also in one COSBOA submitted recently to the Attorney General's Office's Privacy Act Review, Small business needs more education, support and resources to ensure the cyber technology ecosystem at grass roots level is as robust as the larger business corporate sector.

3.4.3 Evidence

Small business are key players in the economy and the wider eco-system of firms. Enabling them to adapt and thrive in a more open environment and participate more actively in the

digital transformation is essential for boosting economic growth and delivering a more inclusive globalisation. [1]

Small business contributions depend on their access to strategic resources, such as skills, knowledge networks, and finance, and on public investments in areas such as education and training, innovation and infrastructure.

Small business participation in the knowledge-based economy is held back by skills shortages, poor internal management practices and low levels of workforce training.

3.3.4 Recommendations

CyberWarden as a Scale-able Solution

The micro-strategy principles encapsulated in CyberWarden has the potential for scalability to larger sized entities and the development of a cohesive macro approach.

Leverage Investment in Small Business Cyber Security, as a demonstration of Australia's commitment to a mandated cyber security strategy

COSBOA driven 89 Degrees East developed CyberWarden solution will result in tangible economic and social development benefits.

89 Degrees East's own submission to this review corroborates that CyberWarden's holistic approach to ensuring its inclusive and comprehensive commitment to cyber security is World leading.

Investment in CyberWarden's national roll-out as a certification-based solution will set a new standard for micro market players, and will formalise the pivotal role they play in any first or developing world economy,

[1] https://www.oecd.org/industry/C-MIN-2017-8-EN.pdf

5. Conclusion

In conclusion, while remaining concerned regarding the potential impact of complex regulatory reforms on Small businesses, COSBOA acknowledge and appreciates the Government's aspirations for, and commitment to, strengthening cyber security laws and compliance frameworks.

COSBOA recommends through its CyberWarden program, a supportive approach that empowers Small businesses that will enable the Government to realise its best practice goal of being the most cyber safe country in the World.

Lastly, to ensure well-informed and effective policy development, COSBOA strongly advocates for ongoing consultation with small business stakeholders.

On behalf of our members, we sincerely thank you for the opportunity to participate in this consultation process.

Yours sincerely,

Matthew Addison
Chair of the Board
Council of Small Business Organisations Australia (COSBOA)

Secretariat: PO Box 463 Canberra ACT 2601 (+61) 493 364 720 Our advocacy team is based in Canberra Email: ceo@cosboa.org.au/www.cosboa.org.au