Australian Retailers Association

SUBMISSION
CYBER SECURITY STRATEGY 2023-2030

APRIL 2023

EXECUTIVE SUMMARY

The Australian Retailers Association (ARA) welcomes the opportunity to provide comments to the Expert Advisory Board tasked by the Minister for Home Affairs and Cyber Security to develop Australia's Cyber Security Strategy (the Strategy).

We also support the Government's commitment and investment to make Australia the most cyber-secure country in the world by 2030 and are equally committed to ensuring that the retail community builds its cyber security capability and preparedness in coming years.

Our submission makes a number of observations and recommendations in response to the Discussion Paper released by the Expert Advisory Board. We look forward to further engagement as design of the Strategy is finalised and implementation commences.

INTRODUCTION

The ARA is the oldest, largest and most diverse national retail body, representing a $400 billion sector that employs 1.3 million Australians – making retail the largest private sector employer in the country. As Australia's peak retail body, representing more than 120,000 retail shop fronts and online stores, the ARA informs, advocates, educates, protects and unifies our independent, national and international retail community.

We represent the full spectrum of Australian retail, from our largest national retailers to our small and medium sized members, who make up 95% of our membership. Our members operate across the country and in all categories - from food to fashion, hairdressing to hardware, and everything in between.

The ARA strongly supports the Government's commitment to make Australia the most cyber-secure country in the world by 2030 and offers the following overarching recommendations:

- The Strategy should aim to empower Australian businesses with the tools and information they need to keep customer data safe from cyber threats.
- The Strategy should favour education and provision of best-practice guidance models over legal obligations and a strict enforcement framework.
- The Strategy should outline design principles to ensure that any new regulation is fit-for-purpose and proportionate to the risk being addressed.

RESPONSES TO THE DISCUSSION PAPER

We offer the following responses to the questions in the Board's Discussion Paper that are most relevant to the Australian retail sector.

Australian Retailers Association (ABN 99 064 713 718)
Level 1, 112 Wellington Parade, East Melbourne VIC 3002

Australian Retailers Association

What is the appropriate mechanism for reforms to improve mandatory operational cyber security standards across the economy?

The ARA prefers regulatory guidance rather than the creation of more legislation and regulation, because we believe this approach is more flexible and adaptive to future developments than black letter law interventions. We also believe that any intervention should be supported by a significant investment in education measures to help build capability and preparedness across the sector.

Is further reform to the Security of Critical Infrastructure (SOCI) Act required? Should this extend beyond the existing definitions of 'critical assets' so that customer data and 'systems' are included in this definition?

In principle, the ARA is supportive of including customer data as a new asset class under the SOCI Act.

However, it is not clear whether including customer data as a critical asset would increase the number of organisations covered by the SOCI Act, or simply increase the compliance burden on companies already obligated under the Act. Amongst our membership, Coles and Woolworths are considered critical food and grocery assets but we concede that the purpose of this proposal could be to expand the number of retailers with future obligations in respect of customer data.

If the impact of this change does increase the number of organisations with a compliance obligation under the Act, we are concerned that this would create an onerous and unnecessary burden for retailers, the vast majority of which collect and are responsible for customer data. In the digital age, even the smallest retailers collect customer data but not to the scale that a breach of their systems would affect a large number of Australians and necessitate government intervention, as was the case with notable data breaches in 2022.

We note that existing regulation already protects customer data. The Privacy Act (1988) requires entities to take reasonable steps to prevent customers' personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure, as well as requiring entities to report breaches to the Office of the Australian Information Commissioner (OAIC) and affected individuals. We also note that the government is considering reforms to the definition of personal information under this Act to cover more types of customer data.

Nonetheless, we understand that there is merit in giving the government the power to intervene in large scale cyber-attacks affecting the customer data of millions of Australians, such as those that occurred last year.

The ARA therefore recommends that, if customer data is included in the definition of critical assets, it only applies to entities that hold sufficient data that a breach of their systems would constitute a nationally significant event. In setting an appropriate threshold, consideration should be given to the number of individuals about whom data is held and the type of data held, noting that some information is more sensitive and presents a higher risk if compromised.

We also note that how the data is held can also make a difference. For example, a list of Medicare numbers alone may not be useful, but if it can be easily matched to names and addresses it poses more of a risk in terms of potential misuse if it is stolen.

Should the obligations of company directors specifically address cyber security risks and consequences?

The ARA is not in favour of discrete obligations on company directors in respect of cyber security. Directors already have responsibilities to ensure good governance on behalf of shareholders and our assumption is that

Australian Retailers Association (ABN 99 064 713 718)
Level 1, 112 Wellington Parade, East Melbourne VIC 3002

these obligations would extend to cover cyber security as a key strategic, operational, reputational and compliance risk.

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?

The ARA recommends ongoing consultation with the business sector to monitor the regulatory burden on the private sector in terms of cyber security. Industry experts will be best placed to work with government to identify opportunities to streamline the framework and avoid unnecessary duplication.

More specifically, we suggest that more work could be done to clarify reporting obligations when a company is responding to an immediate threat or breach. While we understand that it is critical that companies report incidents at the earliest opportunity, we recommend that the framework promotes open communication during an incident and that reporting obligations are not such that company resources are unnecessarily diverted from dealing with the immediate threat.

In terms of opportunities to streamline existing regulatory frameworks, we note the success of National Coordination Mechanisms over the past few years that served to coordinate a whole of government response, without circumventing the powers of any one regulator involved in that response.

Should the Government prohibit the payment of ransoms and extortion demands by cyber criminals?

The ARA is supportive of discouraging victims of cybercrime from paying ransoms and extortion demands with the intention of sending a strong message to criminal actors.

However, any legal prohibition would need to be complemented by measures to uplift capability and reduce the risk of cyber-attacks, with support available to businesses targeted by cyber criminals to minimise the impact of data breaches.

The ARA is well placed to work with the government to promote awareness across the retail sector about how best to respond to ransomware and extortion threats. The ARA oversees the ARA Retail Institute, a Registered Training Organisation with 30 years' experience upskilling the retail community and would be interested in working with government to develop micro-credentials and training programs in this area for our members.

Does Australia require a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda?

The ARA recommends that cyber security be embedded across the education system rather than taking a siloed approach. However, we recognise that business may have a preference to upskill in a more discrete manner to suit their requirements and circumstances.

In an ideal scenario, any employee who uses a connected device would have basic cyber security skills. As above, the ARA could play a positive role in building awareness and capability across the sector through the ARA Retail Institute.

In our pre-budget submission to Treasury, we also recommended that the government make further investment to help accelerate the roll-out of the Cyber Wardens Program.

Australian Retailers Association (ABN 99 064 713 718)
Level 1, 112 Wellington Parade, East Melbourne VIC 3002

Should the government respond to major cyber incidents (beyond existing law enforcement and operational responses) to protect Australians? Should government consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators?

The ARA supports the establishment of a single national coordinator for cyber incidents to streamline reporting processes and facilitate efficient communication between regulators. This centralised point of contact would enable businesses to report cyber incidents through a single portal, thereby harmonising existing requirements and reducing inefficiencies.

To encourage transparent information sharing, it is essential that this portal provides a safe environment, where businesses should be able to disclose sensitive information without fear of prejudice or immediate punitive action. The primary goals of this portal should be to support government efforts in investigating cybercrimes and helping to coordinate a whole-of-government response to support impacted businesses, not penalising businesses for being the unfortunate target of malicious actors.

Given its enforcement responsibilities, we do not think that the OAIC should manage this portal. By separating the enforcement and investigative aspects from the cyber incident reporting process, it would create a more conducive environment for cooperation between the government and businesses in addressing major cyber threats.

How can government and industry work to improve cyber security best practice knowledge and behaviours, and support victims of cybercrime? What assistance do small businesses need from government to manage their cyber security risks to keep their data and their customers' data safe?

Recent breaches have demonstrated that even large, well-resourced corporations can be vulnerable to cyber security attacks. It is therefore paramount that all businesses, large and small, invest in digital capabilities.

When providing assistance for small retailers, the ARA makes the following recommendations.

- Avoid making cyber security a separate topic or issue. Incorporate cyber security information into guidance and education for other digital skills, for example building a website, selling products online, and using a customer relationship management system.
- Provide accessible pathways for small business to engage with government. The ARA's experience is that small retailers do not always know how and when to engage with government. When delivering cyber security information, use the channels already used by small retailers, such as industry associations and business advisers. The ARA is well placed to support government in sharing information with members.
- Offer cyber security training to those service providers who already advise or work with small retailers, such as accountants, bookkeepers, IT professionals and website developers.

CONCLUSION

The ARA appreciates the opportunity to provide feedback on the Strategy. We look forward to further engagement with government and the Expert Advisory Board on these important changes.

For any questions about this submission please contact [redacted]

Australian Retailers Association (ABN 99 064 713 718)
Level 1, 112 Wellington Parade, East Melbourne VIC 3002