ARA SUBMISSION

AMENDMENTS TO THE SECURITY OF CRITICAL INFRASTRUCTURE ACT 2018 (CTH): DRAFT IMPACT ANALYSIS

MARCH 2024

The Australian Retailers Association (ARA) welcomes the opportunity to provide comments on Amendments to the Security of Critical Infrastructure Act 2018 (Cth): Draft Impact Analysis (IA).

The ARA is the oldest, largest and most diverse national retail body, representing a $420 billion sector that employs 1.4 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 and international 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.

EXECUTIVE SUMMARY

This submission advocates for Option 3 (outlined in the Draft Impact Analysis) as the preferred approach to address critical infrastructure challenges faced by our members in the food and grocery sector. Option 3 entails enhancing collaboration between industry and government through the Trusted Information Sharing Network (TISN), without necessitating regulatory changes to the Security of Critical Infrastructure Act (SOCI Act).

In respect of this submission, the ARA is proud to represent Australia's largest supermarket brands who are key stakeholders in the TISN Food and Grocery Sector Group (FGSG).

The ARA submission responds to three options outlined in the consultation paper, with a short summary of ARA's position on the three options below.

Option 1 (Maintaining the status quo)
This option fails to address identified gaps in the SOCI Act and leaves critical infrastructure assets vulnerable to growing threats.

Option 2 (Regulatory change)
Option 2 imposes regulatory burdens and compliance costs on our members. Concerns arise regarding potential disruptions to operations and supply chains.

Option 3 (Enhanced collaboration with industry)
This option fosters collaboration and information sharing between industry stakeholders and government.

- By leveraging the TISN, Option 3 enables industry-led responses to incidents, enhances post-incident resilience and promotes flexibility in risk management approaches. This approach is a good first step as industry and government better educate themselves on cybersecurity.
- While acknowledging the potential costs associated with Option 3, including investments in engagement and compliance efforts through the TISN, this submission emphasises the potential for increased industry resilience and preparedness in the face of cybersecurity threats.
- Option 3 offers flexibility for entities to tailor risk management approaches to their specific needs, promoting industry autonomy and responsiveness.

DISCUSSION

The Problem

1. **Is the problem set out in the discussion paper accurately described in relation to your entity? Are there other elements of the problem which have not been mentioned in the IA?**

   The problem outlined in the consultation paper accurately reflects the challenges faced by retailers in safeguarding their critical infrastructure against cyber threats. Retailers are increasingly at risk of being targeted by cybercriminals due to the vast amounts of sensitive customer data they store and their interconnected systems. However, there are additional elements specific to the retail sector that warrant consideration:

   Supply chain vulnerabilities: Retailers rely heavily on complex supply chains involving numerous partners and vendors. Each node in the supply chain presents a potential entry point for cyber threats, necessitating comprehensive risk management strategies across the entire ecosystem.

   E-commerce platforms: Retailers face unique challenges in securing their e-commerce platforms against cyber threats. The increasing reliance on online sales channels makes these platforms lucrative targets for cybercriminals. Retailers must navigate the complexities of securing their e-commerce infrastructure while ensuring seamless customer experiences. However, any government intervention should aim to support retailers in enhancing cybersecurity measures without imposing impractical or overly burdensome regulatory requirements. It's essential to strike a balance between regulatory compliance and operational feasibility to effectively mitigate cybersecurity risks in the e-commerce sector.

   Emerging technologies: The adoption of emerging technologies such as Internet of Things (IoT) devices, artificial intelligence (AI), and cloud-based services introduces new cybersecurity risks. Retailers must navigate the complexities of securing these technologies while leveraging their benefits to enhance customer experiences and operational efficiency.

   Willingness to cooperate: Retailers have demonstrated the ability to work collaboratively through industry groups and with government. Such collaboration was enabled during the COVID-19 pandemic by an ACCC authorisation and facilitated through the National Co-ordination Mechanism. Given retailers willingness to collaborate, we consider that government intervention should focus on *authorising* collaboration and activity, rather than directing retailers to take particular action. This would reduce the overhead on government and retailers in shaping directions and consequently reduce the cost of response.

2. **Do you have any key examples from your experience which demonstrate or mitigate the significance of the identified problem?**

   Data breach incident: A prominent retail chain experienced a data breach wherein hackers gained unauthorised access to customer database, compromising millions of personal records. The incident resulted in financial losses and reputational damage for the retailer. Subsequent investigations revealed vulnerabilities in their cybersecurity infrastructure, prompting the implementation of enhanced data protection measures and incident response protocols.

   Supply chain disruption: A cyber attack targeting a port operator saw the operator temporarily take servers offline to contain the risk, with disruptions to supply chain operations. The disruption held up some 30,000 cargo containers, leading to inventory shortages and delivery delays. Retailers with robust supply chain resilience strategies in place were better equipped to mitigate the impact of the disruption by quickly identifying alternative suppliers and communication channels to minimise customer inconvenience.

OPTION 1 CONSULTATION QUESTIONS

3. Are the impacts of Option 1 accurately described as related to your entity?

The impacts of Option 1 outlined in the discussion paper accurately reflect the potential consequences for our members. Maintaining the status quo poses risks and vulnerabilities to operations, particularly in relation to critical infrastructure security and resilience.

4. What do you consider would be the most material costs to your entity of Option 1?

The most material costs to our members under Option 1 would stem from the heightened exposure to all-hazard threats. The ARA supports more regular collaboration with government that helps our members to fully understand the risks before a cyber attack impacts their business, rather than until they have experienced an attack firsthand.

Educating our members, not just those impacted by the SOCI Act but even more broadly would greatly protect our members and more importantly their customers, from cyber threats. Specifically, the risks associated with cybersecurity breaches, operational disruptions and compromised infrastructure pose significant financial, reputational and operational challenges.

5. Are there any other impacts (negative, positive or neutral) arising from the status quo which have not been mentioned in the IA?

In addition to the impacts, maintaining the status quo may lead to several other consequences.

Negative Impacts:

- Increased susceptibility to emerging cyber threats and sophisticated attacks due to stagnant regulatory frameworks.
- Limited ability to adapt to evolving risks and technological advancements, potentially hindering innovation and competitiveness.

Positive Impacts (from maintaining the status quo):

- Continuity in existing operations and regulatory compliance procedures, minimising disruptions and transition costs.
- Retention of flexibility in addressing cybersecurity and risk management practices tailored to our members' specific needs and circumstances.

Neutral Impacts:

- Continued reliance on internal cybersecurity measures and risk mitigation strategies without external regulatory mandates.

OPTION 2 CONSULTATION QUESTIONS

6. **Will a requirement to capture 'business critical data' in your risk management activities have a material impact on staff effort, capital expenditure, or operating costs? If so, what do you estimate will be the marginal cost increase for your entity?**

   The ARA acknowledges the necessity of capturing 'business critical data' in risk management activities but we also anticipate that our members are likely to incur material incremental costs as a result of meeting this requirement.

   There may be some impact on staffing and operational processes and we foresee an increase in capital expenditure and operating costs to meet this regulatory obligation. Infrastructure and processes may require continual upgrades or investments to ensure compliance with the expanded definition.

   Therefore, while staff time dedicated to compliance efforts may contribute to the overall cost increase, the primary financial implications are expected to stem from the need for substantial investments in technology, systems and training to align with the amended definitions.

7. **Are there any other impacts arising from Measure 1 which have not been mentioned in the IA?**

   The ARA is not aware of any other impacts.

8. **Are the categories of costs identified an accurate representation of the impact of a direction/s?**

   The categories of costs outlined in the hypothetical scenario for Measure 2 provide a broad overview of potential financial implications for our members arising from a direction being issued. However, while these categories capture significant aspects such as ongoing uplift in cyber defences, ransom demands, and loss of research and development capability, they may not fully encompass all potential costs incurred by our members.

   For example, increased costs related to government relations, legal consultations, management resources, and loss of productivity during incident response are not explicitly addressed in the initial categories. Although our affected members may already have existing resources, cybersecurity demands specialists who have some expertise in the field and can swiftly grasp the complexities involved, especially during a cyber attack when prompt decisions are imperative.

   Therefore, while the identified costs offer valuable insights, a more comprehensive analysis that considers a broader range of potential expenses would provide a more accurate representation of the overall impact of a direction on our members in the food and grocery sector.

9. **Are there other scenarios which you foresee as arising under a consequence management power, and would like government to consider in this IA?**

   The ARA supports scenarios where our members could enhance their internal capabilities to facilitate better collaboration with the government in the event of an attack. Rather than imposing regulatory requirements, we believe that businesses are best positioned to understand their operations and tailor their responses accordingly.

   By investing and building robust capabilities within their teams, our members can foster a proactive approach to cybersecurity and effectively contribute to coordinated efforts with government agencies during

crisis situations. This approach not only promotes flexibility and agility but also ensures that responses are aligned with the specific needs and challenges faced by individual businesses within the sector.

10. Do these costs reflect the impact a direction of this kind may have on your entity?

As per our previous response, we believe that cybersecurity demands specialists who have some expertise in the field. So, while our members may have their own capabilities in place, there will be an additional requirement to hire staff with some knowledge and understanding in this field.

11. Do the average costs outlined in the three examples align with your expectations of costs which may be incurred by your entity if issued a direction?

While we acknowledge the efforts made to estimate potential costs associated with ministerial directions, it's essential to recognise the inherent uncertainty surrounding the full impact of such directions.

As representatives of the food and grocery sector, our primary concern is ensuring the resilience of our industry in the face of cyber threats. Overregulation, especially without a comprehensive understanding of the sectors' intricacies, could lead to unintended consequences and hinder our ability to effectively respond to cyber events.

Moreover, introducing directives that place restrictions on who businesses can contract may inadvertently disrupt supply chains and drive up the prices of goods. This uncertainty surrounding government control over business contracting decisions could exacerbate challenges during cyber incidents.

Therefore, we advocate for a cautious approach that prioritises collaboration and flexibility over rigid regulatory measures.

12. Are the costs of Measure 2 accurately described as related to your entity?

While Measure 2 may not directly impose costs on all regulated entities, it is important to recognise that our members may experience financial implications. As highlighted in previous discussions, cybersecurity requirements demand specialised expertise, particularly during high-stress situations like cyber attacks where rapid decision-making is crucial.

Therefore, the costs associated with Measure 2 would extend beyond compliance with directives to include the procurement of cybersecurity experts and resources necessary to address the complex challenges posed by cyber incidents.

13. What do you consider would be the most material costs to your entity of Option 2 (when considering any marginal impact on staff effort, capital expenditure, or operating costs)?

The most material costs to our members concerning Option 2 would likely stem from the potential implementation of directives issued by the government. While specific costs may vary depending on the nature and scope of the directions, we anticipate that additional resources would be required to comply adequately.

These costs could be avoided if government authorised behaviour (allowing retailers to take action as they saw fit) rather than directing a specific course of action, which would require significantly more engagement and consequently cost to business.

These costs may include additional staff effort to address cybersecurity vulnerabilities, potential capital expenditure to upgrade IT and operational technology security, as well as ongoing operating costs associated with enhanced risk management processes.

14. Are there any other impacts arising from Measure 2 which have not been mentioned in the IA?

Beyond the direct costs associated with compliance, there is a concern regarding the potential for unintended consequences resulting from government intervention.

While safeguards and oversight mechanisms are intended to mitigate this risk, there remains a possibility of disruptions to our operations or supply chains. Additionally, the imposition of directives may introduce uncertainty and complexity, which could impede our ability to adapt and respond effectively to cyber incidents.

It's essential to emphasise the importance of ongoing consultation with industry stakeholders to ensure that any measures implemented under Measure 2 strike the right balance between regulatory intervention and industry autonomy.

15. Are the costs of Measure 3 accurately described as related to your entity?

The ARA express our reservations regarding Measure 3, which proposes the introduction of a formal, written directions power to rectify deficient Risk Management Plans (RMPs).

While we acknowledge the importance of cybersecurity preparedness, we believe that the anticipated costs associated with Measure 3 may not align with the interests and operational requirements of our members.

The proposed review and remedy power would not change our members approach to preventative risk as it is in their best interest to protect CI asset(s).

16. If issued a direction to rectify a deficient RMP, will there be a material impact on staff efforts, capital expenditure, or operating costs? If so, what do you estimate will be the marginal cost increase for your entity?

In the event of a direction to rectify a deficient RMP, we anticipate a significant material impact on staff efforts, capital expenditure and operating costs within the retail industry.

The imposition of additional regulatory requirements could strain already limited resources, leading to heightened operational challenges and reduced competitiveness. The marginal cost increase for our entity would likely be related to staff training, technology upgrades, and compliance monitoring.

17. Are there any other impacts arising from Measure 3 which have not been mentioned in the IA?

Beyond the direct financial implications, Measure 3 poses broader risks to industry innovation and competitiveness.

The rigid regulatory framework proposed under Measure 3 may inhibit the adoption of emerging technologies, hindering the retail sector's ability to adapt and thrive in a rapidly evolving digital landscape.

Moreover, increased regulatory oversight could undermine trust and collaboration between industry stakeholders and government agencies, impeding efforts to address cybersecurity challenges

collaboratively. As such, we urge the government to explore alternative approaches that prioritise industry engagement and voluntary cooperation, rather than imposing regulatory mandates.

At a minimum, any directions to address seriously deficient elements in RMPs must be issued following close consultation. Any directions should clearly define seriously deficient elements and must be supported by a risk methodology that is agreed to by industry. The entity should be given a written notice that states the intended direction, reasons for the direction and invite the entity to respond and engage with the regulator within an agreed reasonable timeframe.

18. Are the benefits of Option 2 accurately described as related to your entity?

The ARA acknowledges the importance of ensuring the reliability and security of critical infrastructure to support Australia's prosperity.

However, we do not believe that the benefits of Option 2, as described, align closely with the interests and operational realities of our members. While Option 2 aims to provide support from the government to coordinate incident responses and flexibility in addressing evolving threats, the retail sector faces unique challenges and priorities that may not be adequately addressed by these measures.

Our primary concern lies in the potential burden of compliance and the impact on operational efficiency, which may outweigh the perceived benefits for our industry. Furthermore, this direction may impact other SOCI sectors that support the operations of our members' core business like freight.

19. What do you consider would be the most material costs to your entity of Option 2?

The most material costs of Option 2 would likely stem from the need to invest in enhanced cybersecurity measures and compliance efforts. This may include expenditures related to upgrading IT and operational technology security systems, training staff in cybersecurity protocols, and ensuring compliance with new regulatory requirements.

Additionally, the potential loss of productivity during incident response and the associated opportunity costs could impose significant financial burdens on retailers.

20. Are there any other impacts (negative, positive, or neutral) arising from Option 2 which have not been mentioned in the IA?

While Option 2 aims to improve incident avoidance mechanisms and support the mitigation of impacts after an incident occurs, there are several potential impacts that warrant consideration. One negative impact could be the increased regulatory burden placed on retailers, leading to higher compliance costs and administrative overhead.

Moreover, the introduction of new security standards and regulatory requirements may require retailers to divert resources away from core business activities, potentially hampering innovation and growth in the sector. The impact of Option 2 on the retail sector remains uncertain and requires careful assessment to ensure that the benefits outweigh the costs for our industry.

OPTION 3 CONSULTATION QUESTIONS

21. Are the impacts of Option 3 accurately described as related to your entity?

The ARA supports Option 3, which involves enhancing collaboration between the government and industry through the established TISN.

This option aligns closely with our recognition on the need for better collaboration and communication channels between government agencies and the retail sector.

During the COVID-19 pandemic, we found that strong communication and collaboration between industry and government were essential for navigating challenges effectively. Therefore, Option 3, which focuses on increasing engagement and sharing guidance materials, reflects our belief in the importance of fostering a collaborative approach to addressing critical infrastructure issues.

22. What do you consider would be the most material costs to your entity of Option 3?

Material costs associated with Option 3 would likely stem from the investments required to enhance engagement and compliance efforts through the TISN.

This may include costs related to participating in webinars, workshops, and other collaborative activities facilitated by the TISN. Additionally, there may be expenses associated with implementing any recommended cybersecurity measures or risk management strategies outlined in the guidance materials distributed through the TISN.

While these costs are expected to be relatively low compared to regulatory compliance under Option 2, they are still important considerations for our industry.

23. Are there any other impacts (negative, positive, or neutral) arising from Option 3 which have not been mentioned in the IA?

One additional positive impact of Option 3 is the potential for increased industry resilience and preparedness in the face of cybersecurity threats and other hazards.

By encouraging collaboration and information sharing between industry stakeholders and government agencies, Option 3 can help our members better understand and mitigate risks to critical infrastructure. Moreover, the voluntary nature of Option 3 provides flexibility for entities to tailor their risk management approaches to their specific needs and risk appetites.

However, it's important to acknowledge that Option 3 may also pose challenges in terms of ensuring widespread industry engagement and compliance with the guidance materials distributed through the TISN. Therefore, ongoing efforts to promote participation and facilitate effective communication channels will be crucial for maximising the benefits of Option 3 for our members.

CONCLUSION

The ARA supports Option 3 as the preferred choice for addressing critical infrastructure challenges in the retail sector, aligning closely with the sector's priorities and operational realities.

By enhancing collaboration and information sharing, Option 3 promotes industry resilience, supports effective incident responses, and fosters flexibility in risk management approaches, ultimately contributing to the sector's long-term sustainability and prosperity.

The ARA looks forward to continually engaging in the consultation process with government to ensure a cybersafe Australia.

Thank you for the opportunity to provide a submission on this matter. Any queries in relation to this submission can be directed to our policy team at policy@retail.org.au.