COUNCIL OF SMALL BUSINESS ORGANISATIONS AUSTRALIA

Secretariat: PO Box 463
Canberra ACT 2600

0493 364 720

Our advocacy team is based in Canberra

Email: [redacted]
www.cosboa.org.au

Cyber Security Reforms
Department of Home Affairs
By email: AusCyberStrategy@homeaffairs.gov.au

12 March 2024

Dear Cyber Security Legislative Reforms team,

The Council of Small Business Organisations (COSBOA) thanks the Department of Home Affairs for its continued consultation on the proposed legislative reforms and welcomes the proposed reforms in line the with Government's commitments in the 2023-2030 Australian Cyber Security Action Plan.

Introduction

COSBOA has continued to emphasise the importance of accessible, affordable, achievable, and manageable cyber security measures for small businesses. This includes recommendations that government focus on educating and upskilling small businesses to empower them to take ownership of cyber security, rather than imposing complex reporting and penalty regimes. Small businesses are often poorly positioned to tackle cyber incident reporting requirements, with many remaining confused about what they are expected to do when an incident occurs. The proposed reforms touch on resolving some of these issues.

The comments below are aimed at addressing the questions proposed by the consultation paper under each relevant measure.

Measure 1 – Helping prevent cyber incidents – secure by design standards for Internet of Things (IoT) devices.

The Consultation Paper asks who in the smart device supply chain should be responsible for complying with a proposed mandatory cyber security standard. The party responsible for organising the operating system should be responsible in ensuring that their product meets the mandatory cyber security standards. However, as highlighted by Government in the Paper, any regulation on IoT devices should only be used as a last resort and must demonstrate a net benefit to society. It must not be lost to Government that increased costs for businesses to implement regulatory change is likely to end in higher cost of good for the consumer.

COSBOA queries whether a Policy Impact Assessment has been undertaken to determine dollar amount impact and requests this information be shared publicly.

Furthermore, COSBOA has no initial concerns with the first three principles of the ETSI EN 303 645 standard from being adopted in an Australian context, however, as always, implementation of the Standard in general, requires net benefit. If Government decide to replicate multiple standards, then simplicity for duty holders must be ensured so that all obligations are understood and can be met.

All businesses should be given at least 2 years to adjust to new cyber security requirements for smart devices. It is recommended that further consultation regarding the appropriate time frame take place with manufacturers within this industry to better understand product lifecycle and development stages to minimise costs of implementation for the business.

Measure 2 – Further understanding cyber incidents – Ransomware reporting for businesses.

COSBOA considers that the ransomware reporting obligation be limited to specific entities, such as those with an annual turnover of more than $10 million/a year. For businesses smaller than the threshold, guidance material should be provided to educate businesses on protecting themselves against ransomware and cyber extortion. COSBOA's Cyber Wardens program is one example.

Government should also consider the efficiency and productiveness of a two-pronged reporting obligation. Additional time spent by a business in reporting an incident takes away from running the business. Therefore, the Government must develop streamlined and easy to follow reporting options. This can also include Government review of other mandatory reporting schemes to ensure consistency in time frame and approach.

It is of utmost importance that a no-fault and no-liability principle is included in the proposed legislation. Businesses should not be penalised for paying a ransom (when they have already had financial outlay through the ransom payment) by Government. The government can include a due diligence obligation to ensure an entity has taken all reasonable steps to avoid a cyberattack.

Additionally, there are plenty of information sharing obligations across Government that can be used to support national preparedness and victim support measures. New information sharing measures should not be created if current measures can be used. COSBOA would like to see a mapping exercise undertaken by Government to show how any newly proposed information sharing system fits into current practices.

Measure 3 – Encouraging engagement during cyber incidents – Limited use obligation on the Australian Signals Directorate and the National Cyber Security Coordinator

COSBOA is of the view that a prescribed cyber security purpose for a limited use obligation should be aligned with other similar information sharing obligations that already exist within Government, in addition to those suggested in the Paper. The information gathered should then be able to assist government in ensuring future instances of cyber-attacks do not occur, and that businesses are supported with the appropriate resources to safeguard themselves

from harm. Government should also consider incentives that related to a business's cyber health in general.

Measure 5 – Protecting critical infrastructure – Data storage systems and business critical data.

Research by AUDA, 89Degrees East and COSBOA in 2022 found that the majority of small businesses (58%) stated that the owner of the business has responsibility for IT, and there isn't anyone specific with this level of responsibility.

The least common cyber security practices amongst small businesses are:

- Giving updates to staff around what to do if a cyber security incident occurs (53% never)
- Having a cyber security plan for handling cyber security incidents (44% never)

Insights from Cyber Warden's research conducted from 2000+ small business owners and their employees showed that 44 per cent had experienced a cyber-attack. 43 per cent of cybercrime targets small business, and it is the top 2 risk reported by small business.

Small businesses do not have the skill or capabilities right now to manage cyber risks. Not only is it costly, but it can be overwhelming. That is why the Cyber Warden's program has been designed to assist small businesses become more cyber aware and safe.

For small businesses who are involved with critical infrastructure, the proposed amendments need to ensure that regulatory burden and complexity isn't enhanced as a result. The Government's current consideration of removing the small business exemption as part of the Privacy Act review will have a huge financial and operational impact on small businesses and their compliance obligation. The Government must ensure that thorough work is done to ensure there is no duplication in responsibilities and that all new obligations are clear, concise and explained in a simple manner.

As mentioned, the financial impact of increased regulatory burden will be high for small businesses already struggling with the cost of doing business. Additionally, if small businesses then also decide to get cyber insurance to further protect themselves, costs again increase. COSBOA recommend that a PIA depicting the costs of the proposed amendments be undertaken and shared with stakeholders.

Conclusion

Ultimately, a balance must be found between tailored and targeted educative services approach, investment in cyber security infrastructure, and achievable approach to cyber security regulatory requirements.

COSBOA is available for further consultation based on our above submission.

Kind regards,

Luke Achterstraat
CEO