10 April 2024

Cyber Security Strategy Division

Department of Home Affairs

6 Chan Street

BELCONNEN ACT 2617

Via online form: Cyber Security Legislative Reforms

Dear Sir/Madam,

Ensuring that cyber security law reforms address the needs of small businesses

Small businesses account for 97.3 per cent of Australian businesses and employ 42 per cent of the workforce, so it is essential for the public interest that cyber security law reforms consider the perspectives and interests of small businesses.

Cybercrime has broad and significant adverse effects on the welfare of small businesses. More than 60 per cent of surveyed small businesses have encountered a cyber incident, and most cyber incidents reported to the Australian Cyber Security Centre (ACSC) are from small businesses.[1] Among cyber incidents reported to ACSC by small businesses in 2022-23, the average loss to the business was $45,965.[2] In addition to financial loss, the ACSC finds that small businesses may also face legal issues or personal health impacts as a result of cybercrime.[3]

Despite the significant cost of cybercrime to small businesses, they generally have limited ability to dedicate staffing and financial resources for cyber security. Nearly half of surveyed small businesses in 2019 spent less than $500 on cyber security each year, and fewer than 10 per cent of surveyed businesses with four or fewer employees outsourced their IT security needs.[4] In a 2023 study, 31 per cent of surveyed Australian small businesses reported reducing their cybersecurity spending in the past year due to rising cost pressures, with 63 per cent claiming that they were actively trying to scale down business costs.[5]

It is therefore important that the proposed legislative reforms enable the Australian Government to protect Australian businesses and consumers from cyber incidents, improve awareness of cyber security risks and mitigation strategies, and appropriately manage additional regulatory burden on small businesses. This may require that obligations for small businesses consider effects on

[1] Australian Signals Directorate (ASD), *Cyber Security and Australian Small Business*, ASD, Australian Government, November 2020, p. 11; ASD, *ASD Cyber Threat Report 2022-2023*, ASD, Australian Government, November 2023, p. 34.
[2] ASD, *Small Business Cyber Security*, Australian Cyber Security Centre website, n.d., accessed 21 March 2024.
[3] ASD, *ASD Cyber Threat Report 2022-2023*, ASD, Australian Government, November 2023, p. 33.
[4] ASD, *Cyber Security and Australian Small Business*, ASD, Australian Government, November 2020, pp. 11, 14.
[5] Mastercard, *New data reveals up to 309,000 Australian small businesses say they've been targeted by cyberattacks, yet many are forced to cut cybersecurity costs* [media release], Mastercard, 6 November 2023, accessed 8 April 2024.

small businesses, the diversity of small businesses, their available resources and the personal information they collect, handle and store.

1. Ransomware reporting obligations should be limited to businesses with more than $10 million annual turnover and 20 or more employees

As the Consultation Paper sets out, it is important to strike an appropriate balance between enhancing visibility of the ransomware threat and reducing additional regulatory burden for businesses.

With some exceptions, small businesses are more likely to collect a smaller amount of sensitive information than their larger counterparts. Small businesses are also more constrained in terms of financial resources and staffing, and can be especially burdened by additional reporting obligations.

With regard to privacy law reform, the ASBFEO has called for a right-sized regulatory approach for small and family enterprises, graduated for assessed risks. This could consist of a checklist approach (or simplified interactive template) of the 13 Australian Privacy Principles (APPs) explaining the clear steps required to meet their privacy obligations, including as controllers and/or processors of personal information. The number and onerousness of compliance steps imposed on a small business should be proportionate to its level of exposure to privacy risk.

The ASBFEO has also recommended incorporating cyber security guidance and Consumer Data Right rules into the actionable steps for small businesses. Including a multifaceted regulatory option would expand on the Privacy Act Review's proposal (10.6) for standardised templates and layouts, and incorporate (or complement) adjacent duties, obligations and support resources. A clear and specific set of actions that a business should take if its information and/or privacy duties are compromised would help a small business to be sure-footed in its response.

While it is crucial to clearly articulate through concise, accessible guidance what small businesses need to do, it is also important to verify when compliance has been successfully completed. This reduces needless uncertainty and anxiety for small business owners; and encourages full and timely compliance. The ASBFEO regards this verification procedure to be a key element of a right-sized approach to privacy regulation.

Consistent with a right-sized and supportive regulatory approach, the ASBFEO supports limiting the application of the ransomware reporting obligations to businesses with more than $10 million in annual turnover. As an additional condition, the obligations should be limited to businesses with 20 or more employees to help ensure that regulatory burden is proportionate to risk and considers the available resources of the businesses affected.[6]

2. The Cyber Incident Review Board should include dedicated members that represent small business interests

The ASBFEO supports establishing a Cyber Incident Review Board (CIRB) to undertake reviews into cyber incidents and share findings and lessons learned with the Australian public.

[6] The Australian Taxation Office defines a small business as an individual, partnership, company or trust that is carrying on a business and has an aggregated turnover of less than $10 million. The Australian Bureau of Statistics defines a small business as an actively trading business with fewer than 20 employees.

The CIRB should include dedicated members that represent small-business interests. This will help ensure that cyber incident reviews consider the needs and challenges affecting small businesses and deliver insights that are relevant to them. This is especially important given that:

- most cyber incidents reported to the ACSC are from small businesses
- many small businesses perceive cyber security as primarily a big-business problem
- the significant costs that small businesses bear in the event of a cyber incident.

3. As part of its reviews and reporting, the Cyber Incident Review Board should provide information on cyber incidents and mitigation tools relevant to small businesses

We acknowledge the useful information available through the ACSC and other agencies to support small businesses to protect themselves from common types of cyber incidents. However, small businesses continue to lack confidence in their understanding of cyber security risks, despite them considering cyber security to be important to their business.[7]

The CIRB, given its unique review powers and functions, should help increase small businesses' understanding of tangible and contemporary cyber security risks and their potential mitigation strategies, by providing actionable insights for small businesses. Such insights can include preventative steps that small businesses can take and advice that holistically considers small businesses' related activities (such as digital engagement, data management and payments).

In providing actionable advice, it would be helpful to illustrate the contribution of human error in cyber incidents and the steps that small businesses can take to prevent common errors or mitigate their harms.[8] Some organisations, including the Victorian Chamber of Commerce and Industry, have focused on simple steps, like multi-factor authentication and turning on live updates, that small businesses can do to protect themselves from cyber incidents.

Another example of how relevant, concise and accessible information on cyber security can be communicated to small businesses is the ASBFEO's cyber security checklist, which is accessible on the ASBFEO's website. The checklist consolidates and provides links to tailored cyber security information and resources for small businesses, produced by government.

If you would like to discuss this matter further, require any further information or would like us to supply small business case studies, please contact the ASBFEO via email at advocacy@asbfeo.gov.au.

Yours sincerely,

The Hon Bruce Billson
Australian Small Business and Family Enterprise Ombudsman

[7] Australian Signals Directorate (ASD), *Cyber Security and Australian Small Business*, ASD, Australian Government, November 2020, p. 5.
[8] As reported by IBM Corporation, human error was a contributing factor to over 95 per cent of studied cyber incidents. IBM Corporation, *IBM Security Services 2014 Cyber Security Intelligence Index*, May 2014, p. 3.