3 September 2021

Department of Home Affairs
6 Chan St
Belconnen ACT 2617

CPA Australia Ltd
ABN 64 008 392 452

Level 20, 28 Freshwater Place
Southbank VIC 3006
Australia

GPO Box 2820
Melbourne VIC 3001
Australia

Phone 1300 737 373
Outside Aust +613 9606 9677
Website cpaaustralia.com.au

By email: techpolicy@homeaffairs.gov.au

Dear Sir / Madam,

Strengthening Australia's cyber security regulations and incentives

CPA Australia represents the diverse interests of more than 168,000 members working in 100 countries and regions around the world. We make this submission on behalf of our members and in the broader public interest.

The key points highlighted in our submission are:

- boards and senior management should have adequate oversight of the cybersecurity posture of their organisation
- organisations should make cyber training mandatory for senior management and directors.
- we favour a mandatory Cybersecurity Labelling Scheme (CLS) to protect consumers. Implementation of the CLS should be considered a high priority

CPA Australia's detailed perspectives on these issues are provided in the attached.

If you have any queries, please do not hesitate to contact Dr. Jana Schmitz, Technical Advisor, Assurance and Emerging Technologies at CPA Australia on jana.schmitz@cpaaustralia.com.au, or Nigel Hedges, Head of Information Security at CPA Australia on nigel.hedges@cpaaustralia.com.au.

Yours sincerely

Dr Gary Pflugrath FCPA
Executive General Manager, Policy and Advocacy

Encl.

Attachment

Governance standards for large businesses

What is the best approach to strengthening corporate governance of cyber security risk? Why?

The lack of adequate governance oversight of cyber risk could result in the loss of customer confidence, reputation damage, potential regulatory action and litigation. To avoid such pitfalls, boards and senior management should have adequate oversight of the cybersecurity posture of their organisation. Alignment of corporate and cyber risk governance practices should be considered a top priority. This will help prioritise and mitigate the range of cyber risk factors with which organisations are confronted.

To strengthen the corporate governance of cyber security risks, the board should:

- set the tone and emphasise the importance of adequate cyber risk mechanisms;
- review the adequacy of budgets allocated for cyber risk management initiatives, training and awareness programs, cybersecurity policies and procedures, and other controls implemented in the organisation;
- be aware of the incident management, disaster recovery and crisis management capabilities of the organisation;
- discuss with senior management how to improve the organisation's cyber risk management capabilities and competencies of staff;
- consider subscribing to an appropriate cyber insurance policy;
- be aware of the "crown jewels" (i.e., critical information systems) of the organisation that must be protected from potential cyberattacks;
- actively engage with chief information officer (CIO), chief information security officer (CISO) and chief risk officer (CRO) on cyber risk management strategy planning and implementation-related activities, and the progress and challenges faced;
- make cyber risk disclosure, as well as IT and privacy risk-related discussions, a regular item on the board's meeting agenda and involve the organisation's cybersecurity executives (e.g., CIOs, CISOs, CROs) in board meetings to discuss potential threats and preventive measures;
- address directors' knowledge gaps in cyber-related areas by attending external training programs and/or having a cybersecurity expert on the board. In this regard, the board should consider whether they would be better served by increasing the entire board's understanding of cyber risk, rather than relying on a single director.[1]

Further, we note that vulnerable business sectors such as banking and financial services should consider having a senior-level cyber risk committee.

[1] Australian Institute of Company Directors (AICD) (2021): Six principles for boards on cyber-risk governance, available at: https://aicd.companydirectors.com.au/membership/membership-update/six-principles-for-boards-on-cyber-risk-governance (accessed 18 August 2021).

Are additional education and awareness raising initiatives for senior business leaders required? What should this look like?

We note that a range of training courses and programs for directors and other senior leaders are available in the marketplace.[2] Such educational courses are useful for increasing cyber literacy and providing directors and senior leaders with the tools and measures useful to mitigate cyber risks. We recommend businesses make cyber training mandatory for senior management and directors.

Mandatory product standard for smart devices

What is the best approach to strengthening the cyber security of smart devices in Australia? Why?

A robust 'co-regulatory approach' involving government, industry and the community is important. We believe that instead of concentrating on government and industry stakeholders only, strong community involvement is also vital to the success of cybersecurity regulation. This is particularly important because of the proposed cybersecurity labelling system.

See our comments on "Labelling for smart devices" below.

Labelling for smart devices

Is a label for smart devices the best approach to encouraging consumers to purchase secure smart devices? If so, should it be voluntary or mandatory?

We favour a mandatory CLS to protect consumers. We note that the Cyber Security Agency (CSA) of Singapore has launched the CLS for smart consumer products to help consumers better understand the cybersecurity provisions these products have to offer. The CLS is voluntary. To encourage adoption of the scheme, CSA waives the application fees for the CLS for one year until 6 October 2021.[3]

Further, we note that a CLS, as proposed by the Australian government, imposes various costs including administration, testing and marketing costs on the manufacturer/business. If a voluntary scheme is adopted, we question whether there will be a large uptake by industry participants because of these costs. Those businesses that do participate are highly likely to pass on those costs to consumers. In turn, this will lead to increased prices of labelled products. Arguably, consumers may decide to purchase cheaper unlabeled alternative products. For these reasons, we believe that the costs should be borne by the government if it decides to adopt a voluntary CLS, at least in the implementation phase.

Internet-connected devices, also referred to as Internet-of-things (IoT) devices have become integral to almost all facets of business and society. However, the security of IoT devices is often an afterthought. Security vulnerabilities have been found in Internet-connected toys, televisions, security cameras, door locks, medical devices, fitness trackers and cars. Criminal actors can use these vulnerabilities to take control over such smart devices, steal and/or

---

[2] See for example, http://aicd.companydirectors.com.au/education/courses-for-the-director/online/online-education/the-boards-role-in-cyber and https://open.uts.edu.au/uts-open/study-area/Technology/business-technology/cybersecurity-for-company-directors-online/ (accessed 24 August 2021).

[3] https://www.csa.gov.sg/Programmes/cybersecurity-labelling/about-cls

manipulate data and spy on consumers. These activities can cause physical, psychological and economic harm, not just to the consumers who own these devices, but also to others who are connected to them.

Further, the increase in the number of people working from home during the COVID-19 pandemic may also provide greater opportunities for criminal actors to get inside poorly-secured home networks, and apply the employee's privileges to get inside their employer's networks, further expanding the threats.

The number of IoT devices worldwide is expected to more than double from 10.03 billion in 2021 to more than 25.4 billion in 2030.[4] Considering these numbers, we favour a mandatory CLS to protect consumers; its implementation should be a high priority.[5]

Should the label be digital and physical?

Manufacturers should equip their products with both a physical CLS and a digital version. It is important that the label is practical to deploy and use and is not burdensome to manufacturers, distributors and consumers.

The label should also be allowed to be displayed in all advertisements and promotional material of labelled products. This includes, but is not limited to, websites and online stores.

[4] https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

[5] IoT devices are used in all types of industry verticals and consumer markets, with the consumer segment accounting for around 60 percent of all IoT connected devices in 2020. This share is projected to stay at this level over the next ten years.