BCA

Business Council of Australia

Strengthening Australia's Cyber Security Regulations and Incentives

Contents

1. About this submission 2
2. Key recommendations 2
3. Overview 3
4. Detailed comments 4
   - 4.1 Setting Clear Expectations 4
     - 4.1.1 Governance standards 4
     - 4.1.2 Minimum standards for personal information 5
     - 4.1.3 Smart Devices 5
   - 4.2 Increasing Transparency and Disclosure 6
     - 4.2.1 Responsible disclosure policies 6
     - 4.2.2 Health checks for small businesses 6
   - 4.3 Protecting Consumer Rights 7
     - 4.3.1 Clear legal remedies for consumers 7
   - 4.4 Other options to lift cyber security 7
     - 4.4.1 Skills 7
     - 4.4.2 Incentivising cyber security investments 8
     - 4.4.3 E-invoicing 8

1. About this submission

This is the Business Council's submission regarding the Commonwealth Government's discussion paper on strengthening Australia's Cyber Security Regulations and Incentives. The Business Council supports government incentivising all parts of the economy achieving good cyber security outcomes.

The Business Council represents businesses across a range of sectors, including manufacturing, infrastructure, information technology, mining, retail, financial services and banking, energy, professional services, transport, and telecommunications.

2. Key recommendations

The Business Council recommends:

1. Voluntary best practice guidance on governance for all businesses be developed for cyber security.
2. The government provides clarity that Directors will not be liable for a cyber security event if the Board has taken reasonable steps to have appropriate cyber security controls in place. In addition, the government should consider the benefits and costs of amending the Corporations Act, to provide certainty for Directors that they will not be liable for losses and damages arising from a ransomware attack if the decision is taken not to make a ransom payment, where the Board has taken reasonable steps prior to the attack to have appropriate cyber security controls in place and could not have reasonably foreseen that those measures would not withstand the ransomware attack.
3. The government bring all levels of industry together to gain consensus and build awareness on the basic cyber security guidance which should be used in all businesses in Australia.
4. Any labelling or product standards for smart devices be led by industry, with government focusing on promoting the recently released IOT Code of Practice and other best practice approaches to securing IOT devices. Ultimately responsibility for labelling must rest with manufacturers (rather than retailers) and must be appropriately "grandfathered" to ensure a transition period for existing stock.
5. Government should undertake further research to assess the efficacy of both the small business health check and the smart device labelling proposals, and particularly whether consumer behaviour will be shifted because of a cyber security trust mark.
6. Measures to attract and retain skilled cyber security workers from overseas be introduced, and these workers be included in any priority cohorts for the purpose of international border restrictions.
7. Support be provided for industry-led skills programs that seek to upskill or retrain existing workers in Australia to move into cyber security careers.
8. The introduction of a minimum digital literacy standard for students in primary and secondary education, including on cyber security.
9. Under the National Careers Institute, make technology, testing, tools, and programs available to students that help them to assess the alignment of different career options with their interests and aptitude, including highlighting potential opportunities in digital or cyber security fields.
10. The introduction of a 20 per cent investment allowance to be applied to purchases of services to lift cyber security and support digital transformation.
11. Government articulate the cyber security benefits of e-invoicing as part of communications with small businesses.

3. Overview

The Business Council welcomes the opportunity to work with government on efforts to lift cyber security across the economy. This is a key issue for all parts of the Australian economy, including business, government, and the community. The Australian Cyber Security Centre has highlighted that malicious cyber activity against Australia is increasing in frequency, scale, and sophistication.[1]

This is reflected in the business community: cyber is at the top of mind for businesses across Australia, with 95 per cent of local CEOs saying cyber is a top threat to growth.[2] Businesses want to improve their cyber posture. We support all portfolios across government working with business to develop and document the best practice approaches and implement positive incentives for all businesses to invest in lifting cyber security practices. Without action the costs from cyber incidents are likely to rise as more economic activity moves online.

As the consultation paper notes, the overall cost of cyber security incidents in the economy is difficult to calculate (the paper notes varying kinds of costs between $316 million through to $29 billion). We look forward to seeing the outcomes of Home Affair's work on the best way to estimate the economic impact of cyber security incidents to Australia. This will be a key part of understanding whether any of the proposed solutions are a net benefit to Australia.

Without this (or other) clear and compelling evidence, it would not be appropriate to put any mandatory requirements in place to lift cyber security. Security by mandate will not keep up with the evolving nature of the threat. Any minimum standards will need to be balanced, to ensure they do not shift what are limited resources from dynamically tackling cyber risks to undertaking compliance activities. Box ticking exercises will be a net negative for both security and economic growth.

As the Department of Home Affairs has highlighted, there are mature businesses with appropriate cyber security controls that are not the intended target of this consultation process. However, some of the potential changes will be felt across the economy, particularly changes to fundamental legislation like the Privacy Act or consumer protections. Any mandatory requirements should be as targeted as possible to limit unnecessary regulatory costs, particularly for those businesses that are not of concern.

Voluntary advice and positive incentives should have wide applicability, however. We support the objective of promoting and advancing the resilience of the entire Australian business community to cyber risks. Best practice guidance and investment incentives will provide all parts of the economy with the knowledge and opportunity to lift their security practices. It will also prevent inequitable outcomes or leaving 'gaps' in the economy still vulnerable to cyber risks.

Government will also need to lead by example, given the critical services they provide and the interactions they have with businesses, large and small, every day. More than a third of all cyber security incidents reported to the ACSC came from Commonwealth and state and territory governments.[3] As the ACSC's *Commonwealth Cyber Security Posture 2020* report highlights, adoption of mandatory cyber standards (ASD's Top Four) remains at low levels across the Commonwealth government, with two-thirds of government agencies self-reporting as being at only an 'ad hoc' or 'developing' level of security; the lowest levels.[4] The ANAO's cyber resilience audit similarly found none of the seven agencies it selected for audit were fully effective in managing cyber security risk, and did not fully meet the mandatory requirements to implement ASD's Top Four.[5] This is despite the Commonwealth government setting a target for government entities to achieve compliance with the Top Four by 30 June 2014. Cyber security is challenging, especially in critical government departments. Lifting cyber

[1] ACSC 2020 https://www.cyber.gov.au/sites/default/files/2020-09/ACSC-Annual-Cyber-Threat-Report-2019-20.pdf
[2] PwC 2021 https://www.pwc.com.au/ceo-agendas/ceo-survey/2021/pwc-australia-24th-ceo-survey.pdf
[3] ACSC 2020 https://www.cyber.gov.au/sites/default/files/2020-09/ACSC-Annual-Cyber-Threat-Report-2019-20.pdf
[4] ACSC 2021 https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/commonwealth-cyber-security-posture-2020
[5] ANAO 2021 https://www.anao.gov.au/work/performance-audit/cyber-security-strategies-non-corporate-commonwealth-entities

security through regulation will be a challenging and costly task, for both the public and private sectors, and it's not clear the benefits of a regulatory approach will outweigh the costs.

Moreover, many large or internationally focused businesses are already looking to comply with requirements in other jurisdictions. Any proposals the government wishes to take forward from this paper should align with international practice to ensure Australia remains an attractive location for investment. This will ensure our continued economic prosperity underpins our wider security. It is encouraging to see the paper references aligning with international standards, and we support this approach.

The discussion paper is seeking feedback across three areas: setting clear expectations, increasing transparency and disclosure, and protecting consumer rights. We provide detailed responses to each of these areas below. Beyond this, the Business Council believes a multi-faceted approach will be needed. We must build on the good initiatives included in the 2016 and 2020 Cyber Security Strategies, including investments in the Joint Cyber Security Centres, funding for law enforcement and the disruption of cybercrime offshore. Beyond the areas identified in the discussion paper, if the government wants to lift cyber security across the economy there are other positive steps government can take, including investment incentives, digital skills, e-invoicing or appropriate rebates on relevant tools and training.

4. Detailed comments

4.1 Setting Clear Expectations

4.1.1 Governance standards

The discussion paper proposes voluntary governance standards for cyber security for larger businesses. It's unclear from the discussion paper what a 'larger business' is or why a voluntary governance standard should only apply to large businesses, when SMEs are equally if not more vulnerable to cyber-attack. We strongly encourage the government to provide clarity on this point, particularly as many are already subject to industry specific standards (such as those set out by APRA), and many larger businesses will be brought into the expanded critical infrastructure regime. Harmonisation of existing industry standards and regulatory frameworks would reduce compliance complexity, allowing governments and business to focus on consistency and resilience uplift.

We recommend that the Department proceed with the development of voluntary best practice guidance on base governance for all businesses and perhaps specify the additional protections or measures expected of larger enterprises. As noted above, cyber security is top of mind for business leaders. General directors' duties already cover care and diligence obligations on cyber risk. This includes for cyber risks. Rather than introducing new obligations, it may be appropriate to consider what these duties mean in practice.

Any guidance that is developed should be applicable to both large and small businesses. SMEs are a key part of the Australian economy. If the focus is on lifting larger businesses' security, cyber criminals will focus their efforts on SMEs, where the relative ability to withstand attack, or more importantly recover from an attack may be greatly reduced.

The discussion paper suggests current laws do not provide sufficient clarity about the levels of appropriate cyber security expectations, and current duties do not incentivise the uptake of uniform cyber security standards. Best practice guidance would provide clarity about expectations. It is critical this is developed in consultation with businesses to ensure it is actionable and applicable. It should also not be out of step with our international partners: if insurance underwriters based overseas can not make sense of our requirements, we may see further withdrawal of director's liability insurance.

If the government is contemplating whether corporate governance appropriately covers cyber security, it may be sensible to consider whether sufficient certainty is provided for directors in responding to attacks like ransomware.

Directors and officers face unique challenges in determining the best approach to ransomware. This includes for director's liability insurance (which may not cover ransomware incidents), and potential conflicts with fiduciary duties (where the most commercially practical approach may be to pay the ransom). Directors may face class actions or other legal risks, including if entities decide against making a ransom payment.

The Business Council supports directors and officers taking responsibility for the businesses they oversee, including appropriately managing risks in a way that best supports and enhances the business for stakeholders. However, even with the best efforts of directors, officers and employees, there will always be a chance that cyber security risks may still materialise.

This creates an impossible situation for directors, who may face legal challenge even where they have made best efforts to mitigate against cyber security risks. The request for advice on how to approach a ransomware or other cyber incident may need to come quickly, in a complex and relatively novel domain without substantial precedents.

For this reason, we recommend the government provides clarity that Directors will not be liable for a cyber security event if the Board has taken reasonable steps to have appropriate cyber security controls in place. In addition, we recommend the government consider the benefits and costs of amending the Corporations Act, to provide certainty for Directors that, in the event of a ransomware attack Directors will not be liable for losses and damages arising from the attack if the decision is taken not to make a ransom payment, provided the Board has taken reasonable steps prior to the attack to have appropriate cyber security controls in place and could not have reasonably foreseen that those measures would not withstand the ransomware attack.

4.1.2 Minimum standards for personal information

The discussion paper asks for views on an enforceable 'Cyber security code for personal information' under federal legislation and suggest this could be made under the Privacy Act.

We do not support the creation of a proposed code under the Privacy Act. Any changes or additions to the Privacy Act should be contemplated as part of the currently ongoing review of the Privacy Act, and not be made in isolation. As the discussion paper notes, the review of the Privacy Act is contemplating whether the Australian Privacy Principles should be amended to provided greater clarity for entities about what constitutes 'reasonable steps' in practice.

Moreover, the Privacy Act affects many entities across the economy, so implementation costs for businesses are likely to be high. However, it excludes key parts of the economy that are most at risk, either because of their capacity to lift security (such as SMEs) or the types of information they hold (such as political parties). The Business Council does not wish to see the creation of excessive regulatory costs for SMEs.

Given we are in the midst of a global pandemic, it would also be sensible for government to consider whether it wants to impose high-cost regulatory intervention where the benefits are unclear. Rather than mandating through a code, we recommend government take the approach recommended by the Cyber Security Strategy Industry Advisory Panel: bringing all levels of industry together to gain consensus and build awareness on the standards which should be used in Australia.

4.1.3 Smart Devices

The discussion paper seeks views on mandatory labelling and product standards for smart devices.

We recommend that any labelling or product standards be led by industry, and that government focus on promoting the IOT Code of Practice and best practice approaches to securing IOT devices. The Code of Practice was only launched in September 2020, and there has not been sufficient time to assess whether the code has been effective. It is still too soon to move to legislation or any mandatory approaches.

As the discussion paper notes, there are steps being taken internationally (such as in the UK) to legislate better practices. If government wishes to act, we support alignment with these requirements. This will ensure we do not create barriers for exporters or lose access to high quality products offered in other jurisdictions.

An industry-led approach will also ensure any proposed approach can account for the wide range of devices which could conceivably fall under the definition of a 'smart device'. This ranges from the devices cited in the discussion paper (smart lights, TVs and baby monitors) through to many cars sold in Australia, which are internet connected. A clear definition of the device in scope will be critical as will clarifying the entitles responsible for labelling the devices.

We support consumers being provided with information they need to make an informed purchase. However, security, and particularly cyber security, is fluid. Researchers are always finding new vulnerabilities. A labelling system may risk giving consumers a false sense of security.

4.2 Increasing Transparency and Disclosure

4.2.1 Responsible disclosure policies

We support the government developing voluntary guidance or toolkits for all levels of industry on the process of development and implementing responsible disclosure policies. This would need to be developed in consultation with industry, and we welcome the discussion paper inviting examples of guidance that currently exists.

4.2.2 Health checks for small businesses

Lifting the cyber security of small businesses in Australia is something members of the Business Council strongly support. We encourage the government to continue to examine ways to support the many small businesses across Australia in lifting their cyber security resilience and posture. However, we wish to see this done in a way that does not unnecessarily drive costs up for small business owners. SMEs need to be provided cost-effective or managed solutions and options to manage their cyber risk.

The discussion paper asks for views on a cyber security health check program for small businesses. This would be a voluntary self-assessment for small businesses, that would check for basic cyber security guidance (such as turning on multi-factor authentication or undertaking regular backups). Small businesses would then be given a trust mark, which could be used to market their business.

We recommend the government undertake further research to assess the efficacy of any health check, and particularly whether consumer behaviour will be shifted because of a cyber security trust mark. Similar research should also be undertaken for the smart device proposals – as the UK based study cited in the discussion paper had a small sample size (less than 60) and may not be representative of Australian consumers. For many larger businesses, particularly in sensitive sectors, minimum cyber security standards are already included in contractual supply chain arrangements. For this reason, a trust mark is unlikely to be a helpful tool for larger businesses in reducing supply chain risks.

Government will also need to consider costs and whether a trust mark may be misleading for consumers. We strongly support any trust mark program be provided as a free service for small businesses. If the program requires payment, then it may falsely signal greater cyber security than its competitors, when in reality it is because they could afford to pay.

As noted above in relation to smart device labelling, a trust mark may also be misleading for consumers, given it only provides assurance of a basic level of security, and does not provide assurance against new or advanced attacks. Cyber security is a continuous journey, not a destination. This makes it substantially different to existing signals like the Made in Australia mark, which does not face adversaries actively attempting to subvert it.

We support government efforts to lift cyber security for SMEs. One alternative may be to offer SMEs such a check as a matter of course as a protective step upon establishing a business, in partnerships with small business commissioners and law enforcement agencies. SMEs could also be encouraged – through appropriate rebates and other measures – to adopt a cyber resilient operating model from the outset. This may be more persuasive in encouraging SMEs to adopt appropriate measures as they have a direct invested interest in protecting their businesses from, for example, the impacts of ransomware. We outline several further proposals at the end of this submission to help with this effort.

4.3 Protecting Consumer Rights

4.3.1 Clear legal remedies for consumers

The discussion paper asks for views on potential gaps in Australian Consumer Law or the Privacy Act in their application to digital products and cyber security risks.

As the paper notes, there is already substantial work underway to consider reforms to the ACL and AGD is undertaking important and long-running work to review the Privacy Act, including consideration of a direct right of action for consumers. We look forward to continuing to engage with these important processes.

We support the approach flagged in the discussion paper of allowing these processes to run their course, which will ensure any changes are considered as part of a holistic reform.

4.4 Other options to lift cyber security

As noted at the outset of this submission, the Business Council welcomes the opportunity to work with government on efforts to lift cyber security across the economy. The initiatives included in the 2020 Cyber Security Strategy were welcome and we have appreciated the collaborative and consultative approach taken by the government in this discussion paper.

The Business Council champions the role that responsible businesses play in generating sustainable economic growth. We consider that most businesses wish to do the right thing by their shareholders, employees, suppliers, and customers, as well as the broader Australian community. Many of the proposals outlined in the discussion paper are about setting or mandating the guard rails for cyber security. In some cases, these will be necessary. However, we also believe positive incentives and removing barriers to businesses achieving good cyber outcomes outcomes will be just as, if not more, effective than mandates.

We outline below several example proposals that will support all businesses (large and small) to achieve positive security outcomes without the impost of regulatory costs.

4.4.1 Skills

One of the main constraining factors for improved cyber security outcomes across Australia is a skills shortage of cyber security professionals.

We strongly support the government looking to build on the critical $90.2 million investment in growing Australia's skills made as part of the 2020 Cyber Security Strategy, as well as subsequent announcements such as the Digital Skills Cadetships trial, which we understand is considering having a cyber security stream. These are vital investments – without a skilled workforce, businesses large or small will not be able to lift their cyber security at any reasonable speed.

In the short term, we encourage the government to consider measures to attract and retain skilled cyber security workers from overseas and include them in any priority cohorts for the purpose of visa approvals and exemptions to international border restrictions. For instance, the government could consider temporarily reverting to four-year visas for all new Temporary Skills Shortage (TSS) visa holders in IT and cyber-related occupations (with continuation subject to a review) to attract globally mobile talent that may be put off by

Australia's quarantine arrangements, limited flights and border restrictions. Longer-term temporary visas will provide more of a pay-off for prospective skilled migrants who are weighing up the costs, inconvenience, and uncertainty, and considering opportunities elsewhere. These visas also provide an easier transition path to permanent residency.

Support should also be provided for industry-led skills programs that seek to upskill or retrain existing workers in Australia with 'job ready' skills and industry placements, to enable them to move into cyber security careers, or lift their cyber capabilities. As society and workplaces evolve in response to technological change, providing all Australians with foundational digital skills will be vital, including for cyber security. We need to look beyond training a minority of cyber security professionals and consider ways to lift the cyber skills of our entire workforce. To aid in this, governments should consider providing guaranteed funding support for foundational skills, including in digital and cyber literacy, delivered through micro-credentialling.

Over the longer term, the Commonwealth should work with states and territories to set minimum digital literacy standards. The Shergold Review of Senior Secondary Pathways highlighted the need for senior secondary schooling to prepare young people for future roles in the workforce and as active and engaged members of civil society. In particular, the report highlighted the need for senior secondary schooling to focus on providing essential foundational skills for every student, including digital literacy. Building on the Shergold Review, there is an opportunity to engage with the start-up community, who are building platforms to support educators in lifting cyber security.

Similarly, students need to be aware of the possible careers that are available. This will mean improving the quality of careers advice and guidance in schools around digital and cyber security industry careers and building on existing initiatives such as School of Life and Year 13. The National Careers Institute can play an important role in this regard.

This will equip students with the skills and awareness of cybersecurity and other digital skills to potentially take up jobs in what is growing area.

4.4.2 Incentivising cyber security investments

Encouraging well targeted investments in technology by all businesses will be vital to lifting cyber security and resilience, avoiding creating pockets or broad sections of vulnerability in the economy, and achieving the government's goal of becoming a leading digital economy by 2030.

Policy settings should encourage all businesses (and government agencies) to shift away from traditional 'capex' approaches to ICT investment. Much of what was previously considered a capital purchase can now be delivered much more cheaply and efficiently on a consumption basis, and – critically – more securely. Using cloud based and SaaS products will allow businesses to take advantage of the 'security at scale'.

However, given many of these technologies are now offered as services (rather than being capital investments), existing support and incentive mechanisms offered by government may no longer be suitable. For SMEs consideration should be given to granting tax incentives, rebates and other mechanisms to promote cyber resilience as a primary point for investment.

We also recommend the government introduce a 20 per cent investment allowance to be applied to purchases of services to support digital transformation. Existing provisions, such as immediate expensing, are not capturing these new forms of investment. This means they aren't enough to encourage businesses to switch to more secure and more productive ways of consuming ICT products.

4.4.3 E-invoicing

The ACSC has identified business email compromise as a common cyber attack vector. As the ACSC describes, this attack involves criminals "fraudulently requesting payment transfers or changing account details on invoices

or payrolls, to redirect funds into bank accounts controlled by the cybercriminal."[6] One of the best ways to reduce this threat will be through the adoption of e-invoicing, which will allow businesses to exchange invoices directly without going via email.

As part of the 2021 Digital Economy Strategy, the government provided $15.3 million to improve awareness of the value of e-invoicing for business and to increase adoption. This is a positive step, and we support the government looking to lift business take up of e-invoicing.

We recommend the government include articulating the cyber security benefits of e-invoicing as part of communications with small businesses. E-invoicing will not be a panacea, so this will need to be done in concert with wider awareness raising of the ACSC's advice on preventing social engineering or impersonation attacks, and how businesses (particularly SMEs) can seek assistance in the event of compromise.

BUSINESS COUNCIL OF AUSTRALIA

42/120 Collins Street Melbourne 3000 T 03 8664 2664 F 03 8664 2666 www.bca.com.au

[6] ACSC 2020 https://www.cyber.gov.au/sites/default/files/2020-09/ACSC-Annual-Cyber-Threat-Report-2019-20.pdf