STRENGTHENING AUSTRALIA'S CYBERSECURITY REGULATIONS AND INCENTIVES

A submission from Australia's leading Corporate ICT and Cyber Secrutiy Training Provider, DDLS.

27th August, 2021

Drafted by Jeremy Daly, Cyber Security Lead DDLS

Sydney Campus
Level 24, 477 Pitt Street
Sydney NSW 2000

Postal
PO BOX K975
Haymarket NSW 1240

DDLS Australia Pty Ltd
ABN 55 133 222 241
ACN 133 222 241

1800 853 276
www.ddls.com.au

Strengthening Australia's cyber security regulations and incentives

Chapter 2: Why should government take action?

1 What are the factors preventing the adoption of cyber security best practice in Australia?

When looking at what factors are preventing the adoption of best practices in Australia, it is imperative to understand some of the challenges organisations face when it comes to cyber security. There are some organisations in industry that have outstanding cybersecurity practices and frameworks, and there are others with minimal or non-existent practices and frameworks. Overall, there is a sense of complacency surrounding cyber-attacks and a belief in many organisations that they will not be the victim of a successful breach. In addition to this, a number of other factors revolving around cost and education come into play, as summarised below.

One of the key challenges is explaining what cyber security best practice actually looks like and how is it measured. While there are many different best practices and standards such as CIS Controls or the Essential 8 that businesses can choose to implement, oftentimes there is not enough education at a board and executive level regarding the level of security within their organisation and their risk of a breach, which can result in a lack of motivation to implement these practices.

Furthermore, there is a lack of understanding at the board and executive levels about the importance of cyber security training for staff, and the significant cyber risk that emerges if organisations do not invest in this area. Additionally, there is a lack of understanding about what specific technology is worth investing in, and many organisations are uninterested in investigating whether their current security systems meet best practice standards. Oftentimes, business requirements, budget, and security needs do not align, which causes organisations to rely on legacy technology and processes and potentially leaves them open to a security incident. The lack of skilled cyber security professionals within organisations who are capable of securing, deploying and managing systems to a best practice level is significantly exacerbating these challenges.

2 Do negative externalities and information asymmetries create a need for Government action on cyber security? Why or why not?

Negative externalities and information asymmetries do create a need for government action. The paper outlines that most buyers don't have the technical capability to determine the security of a product, and those small businesses struggle to find time to understand and address cyber security risks. In the current marketplace, both consumers and businesses struggle to identify, understand and interrogate the security features, output, and lifecycle of a product. Most individuals assume that a security device or solution will be effective straight out of the box, which is not correct in many

instances, thus leaving an individual or consumer potentially vulnerable to a security incident.

Chapter 3: The current regulatory framework

3 What are the strengths and limitations of Australia's current regulatory framework for cyber security?

A key strength within the current regulatory framework is the existence of several laws and regulations that encourage organisations to implement strong cyber security practices, including the *Privacy Act 1988* and Notifiable Data Breaches scheme. However, some organisations find it difficult to comply with these regulations, resulting from a lack of knowledge on what the regulations actually mean; for example, what are considered 'reasonable steps' to protect information as outlined in the *Privacy Act 1988*, or what is considered an 'eligible breach' under the Notifiable Data Breaches scheme.

It can also be challenging for organisations to determine whether or not their current information security principles and frameworks are being implemented within the current regulatory framework, and sometimes this is only discovered once it is too late.

Although Australia has the *Corporations Act of 2001*, where company directors and officers have a duty to act in good faith and with a degree of due care and due diligence when it comes to information security, Australia's regulatory framework does not have the same Accountability, Responsibility and Transparency laws that America's *Sarbanes Oxley* (SOX) has.

SOX requires that all US public companies, boards, management, and public accounting firms be subject to external audit reporting, demonstrating their statement for Attestation Engagements – particularly for the topic of information security, there is a SOC 2 document ensuring companies report on their controls for Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy.

Australian regulations lack this level of requirement, due to the fact that there has never been a local incident similar to the scale of corruption and scandal in US companies such as Enron. Therefore, Australia has not reacted with such a transparent accountability law.

For more information on Trust Services Criteria, please visit the American Institute of Certified Public Accountants document:
https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria.pdf

For some organisations, implementing the Trust Services Criteria can be seen as quite a burden, so the AICPA have recently added a voluntary reporting framework for cybersecurity risk management called SOC for Cybersecurity:
https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/cybersecurityfororganizations.html

4 How could Australia's current regulatory environment evolve to improve clarity, coverage and enforcement of cyber security requirements?

From our position as Australia's leading provider of corporate cybersecurity training, we are constantly being asked, 'What is a reasonable measure for due diligence when working with a third party supplier and evaluating third party, or even fourth party risk?'. Presently, there is no Australian recommendation for this, and local organisations rely on American laws such as SOX for transparency information to make risk-based decisions. A local regulation could be developed by requiring transparency from companies regarding the controls they have in place for information security and determining an acceptable level of control moving forward.

Chapter 4: Governance standards for large businesses

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

The problem with implementing a voluntary or mandatory standard, is that many organisations are already using an array of existing governance models, which all address the integration of cyber security throughout the organisation. If the Australian government was to create (and maintain) a major governance framework, particularly one that may compete with an international framework, this scenario might end up placing unnecessary burden on organisations who already use another governance model. It would be more prudent to enforce that organisation use 'a' governance framework, regardless of which one this is, and give assurances to the implementation of the control objectives within that governance framework.

7 Are additional education and awareness raising initiatives for senior business leaders required?

More education for senior business leaders would be highly beneficial. At a minimum, some level of training on foundational security and understanding the basics of risk, governance and compliance when looking at security within their organisation (if they are not already qualified to do so), would be of strong benefit to them and the organisation. In turn, this would help senior business leaders understand the risks behind not investing in resources and technology to secure their businesses.

Chapter 5: Minimum standards for personal information

8 Would a cyber security code under the Privacy Act be an effective way to promote the uptake of cyber security standards in Australia? If not, what other approach could be taken?

Having a cyber security code under the Privacy Act would be an effective way to promote the uptake of cyber security standards in Australia. If this is implemented correctly, it would also result in an increased level of cyber resilience within organisations. An example of this can be seen with regards to the ATO and its digital

service providers through the utilisation of the Digital Service Provider Operational Framework, which ensures a minimum baseline is implemented for data that is holding PII or PHI information.

Having a data-centric approach would be the most cost-effective way to ensure protection of highly critical or sensitive data within an organisation.

Chapter 9: Health checks for small businesses

23 Would a cyber security health check program improve Australia's cyber security? If not, what other approach could be taken to improve supply chain management for small businesses?

A health check program could be very beneficial, and as outlined in the discussion paper, any small business who completes a health check would benefit from being able to provide additional assurance to their customers and suppliers about their cyber security. It would also help build the businesses own internal cyber resilience and awareness, while simultaneously helping to build a more secure supply chain between industry, small businesses, and consumers.

24 Would small businesses benefit commercially from a health check program? How else could we encourage small businesses to participate in a health check program?

Participating small businesses would benefit from a program like this, as it would essentially build trust with their own customers and suppliers as they would be recognised as meeting relevant cyber health requirements. It is also a good exercise for the owners and employees of these small businesses, as they will receive some training in cyber security awareness and in some cases increase the cyber resilience of their business based on the recommendations.

25 Is there anything else we should consider in the design of a health check program?

To ensure effective engagement and take-up from small business owners, the program needs to be easy to deploy with clear explanations, help and advice to mitigate any issues found. It also needs to be designed and marketed as being beneficial to businesses, in the sense that it will improve their own reputation, and potentially open more business opportunities, by demonstrating they have implemented and met the requirements to pass a security health check.