ForgeRock

ForgeRock Comments on the “Strengthening Australia’s cyber security regulations and incentives” discussion paper issued by the Department of Home Affairs

Reference:
https://www.homeaffairs.gov.au/reports-and-pubs/files/strengthening-australia-cyber-security-regulations-discussion-paper.pdf

August 27, 2021

Global Headquarters 201 Mission St, Suite 2900 San Francisco, CA 94105 +1 415-599-1100

Disclaimer of Liability

While every effort will be made to ensure that the information contained within the document is accurate and up to date, ForgeRock makes no warranty, representation or undertaking whether expressed or implied, nor does it assume any legal liability, whether direct or indirect, or responsibility for the accuracy, completeness, or usefulness of any information.

Global Headquarters 201 Mission St, Suite 2900 San Francisco, CA 94105 +1 415-599-1100

Table of Contents

Global Headquarters 201 Mission St, Suite 2900 San Francisco, CA 94105 +1 415-599-1100

Summary

ForgeRock is pleased to provide our input and thoughts on the discussion paper. We have opted to provide our input to a subset of the questions.

Collaboration between Government, Critical Industries and the Private Sector in general is much needed in an ever growing cybersecurity risk environment. Using standards, guidelines, best practices and enforcing those among all parties is critical for both government, private sector enterprises, infrastructure providers and consumers connecting their devices to public and private infrastructures and services. As our digital environment is, in many aspects, a shared ecosystem it is important that each participant is offered relevant levels of cyber security protections. For an ecosystem as a whole it is also important to reduce the attack surfaces and each participant needs to be able to play their role in that.

Modern IAM solutions are also critical components to consider. Digital identities are used to control connected systems, ranging from end user smart devices, sensors and the portals used to control such systems. It is important that the security of the control plane is considered in combination with the smart devices, sensors and services themselves.

Global Headquarters 201 Mission St, Suite 2900 San Francisco, CA 94105 +1 415-599-1100

Comments on the “Seeking your views” sections

Chapter 2: Why should government take action?

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

   On the high level it can be attributed to education, lack of concise information and to some extent lack of available skills in the market.

   Consumers may not want to know about “cyber security best practises”. Cyber security is simply speaking something they may not want to deal with. They procure a product or a service and expect it to work and do no harm, just like vehicles need to conform to certain standards. A challenge for the industry is to strive for a base level of safety standards, like what is outlined in the discussion paper being reviewed.

   Businesses, especially the larger ones, may have cyber security as a board level topic with associated risk management processes and accountabilities. For this segment it may be easier for the Australian Government to engage and interact as there are dedicated functions in the organisation dealing with cyber security topics.

   For SMEs the focus may be different and the way to reach and inform those segments needs to be different as SMEs may not have dedicated functions in their organisations to deal with cyber security topics.

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

   It does. As an example, consumer orientated connected IoT devices may be exploited to launch attacks on national infrastructures or targeted businesses. An attack on national infrastructure or a critical business may impact citizens. Cyber security action needs to span ecosystems and all stakeholders as everyone connected can suffer the consequences of targeted attacks even if they were not directly targeted. This can be seen as collateral damage, which we

Global Headquarters 201 Mission St, Suite 2900 San Francisco, CA 94105 +1 415-599-1100

need to strive to avoid or minimise.

To state the obvious, possessing information is powerful. If there are parties of a connected ecosystem that are unaware of, let's say, that certain attack vectors exist and other parties don't, harm can be done to the ecosystem as a whole. If you have competing parties in an ecosystem it may be tempting to not disclose information you have to your competitors. From a cyber security point of view an environment of sharing, collaboration and co-ordinated action should be fostered.

Chapter 3: The current regulatory framework

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

   Intentionally left blank.

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

   Intentionally left blank.

Chapter 4: Governance standards for large businesses

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

   Education and information targeted to the private sector with a focus on providers of critical services, manufacturers of critical equipment and their role in our connected ecosystems. In this context critically may vary depending on the stakeholder or consumer.

Global Headquarters 201 Mission St, Suite 2900 San Francisco, CA 94105 +1 415-599-1100

6. *What cyber security support, if any, should be provided to directors of small and medium companies?*

   Easy access to “checklists” that can be consulted regularly and on-demand to help with self assessments.

   Easy access to notifications regarding discovered vulnerabilities and associated mitigation and avoidance strategies.

   Creation of an advisory service or “help line” that can be consulted for advice proactively or during an ongoing incident.

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

   Yes, cyber security is not only an IT issue. It is a whole of business topic, especially as it relates to proactive measures, planning and associated budgeting.

   Online resources in combination with adding the topic of cyber security to business oriented seminars could be one avenue to reach business leaders. To reach a broader business leadership audience the topic of cyber security needs to be exposed outside of core IT and security focused events.

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?*

   As we see the use of various smart devices evolving and becoming a part of our day to day lives and interactions such devices will store, manage and process personal data. Adding a cyber security code under the Privacy Act may provide specific and practical enforcement of how personal data must be managed and protected. This code may be applicable to device and software manufacturers, to service providers processing such personal data and to other parties gaining access to such personal data.

Global Headquarters 201 Mission St, Suite 2900 San Francisco, CA 94105 +1 415-599-1100

9. *What cost effective and achievable technical controls could be included as part of a code under the Privacy Act (including any specific standards)?*

   Active and informed consent collection should always be required.

   The use of open and portable consent receipts, such as Kantara consent receipts to capture a user's authorised use of personal data.

   The use of globally accepted standards, as relevant, similar to what is provided for CDR in the Information Security Profile. I.e., a profile that will ensure that underlying protocols are used according to best security practises.

10. *What technologies, sectors or types of data should be covered by a code under the Privacy to achieve the best cyber security outcomes?*

    The FSI, health government and communications sectors come to mind as they all rely on, create or manage sensitive personal data.

    All types of PII data should be considered.

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

    There needs to be strong efforts to encourage that smart devices are designed according to security and privacy first principles and best practises. It is also important that standardised security mechanisms and associated protocols can be used.

    Associated services, such as cloud based device management, processing of data generated from a smart device etc., also need to be considered in this context. Securing the control plane should be considered as well.

Chapter 6: Standards for smart devices

Global Headquarters 201 Mission St, Suite 2900 San Francisco, CA 94105 +1 415-599-1100

12. *Would ESTI EN 303 645 be an appropriate international standard for Australia to adopt as a standard for smart devices?*
a. If yes, should only the top 3 requirements be mandated, or is a higher standard of security appropriate?

b. If not, what standard should be considered?

Yes, ETSI EN 303 645 can be an appropriate standard. We would encourage that apart from requirements 5.1 - 5.3 that the below requirements also are considered as a matter of priority:

- 5.4 Securely store sensitive security parameters
- 5.5 Communicate securely
- 5.8 Ensure that personal data is secure
- 5.11 Make it easy for users to delete user data

As we indicated in the summary section it is also important to secure the control plane that interacts with smart devices, sensors and services. In that regard we would like to suggest that the TDIF standard for Credential Service Providers, which is based on the NIST 800-63-3 standard, can play an important role in securing access to control plane services.

13. *[For online marketplaces] Would you be willing to voluntarily remove smart products from your marketplace that do not comply with a security standard?*

Intentionally left blank.

14. *What would the costs of a mandatory standard for smart devices be for consumers, manufacturers, retailers, wholesalers and online marketplaces? Are they different from the international data presented in this paper?*

Intentionally left blank.

15. *Is a standard for smart devices likely to have unintended consequences on the Australian market? Are they different from the international data presented in this paper?*

Global Headquarters 201 Mission St, Suite 2900 San Francisco, CA 94105 +1 415-599-1100

A consequence could be that smart device vendors may decide not to enter the Australian market as it may be seen as onerous requirements are placed on them. To counter this, aligning with internationally accepted standards may be desirable and potentially reduce the burden on smart device vendors.

Chapter 7: Labelling for smart devices

16. *What is the best approach to encouraging consumers to purchase secure smart devices? Why?*

    General education and information on the importance of maintaining strong "cyber security hygiene". This will allow consumers to relate to labelling, similar to star ratings for electrical appliances.

17. *Would a combination of labelling and standards for smart devices be a practical and effective approach? Why or why not?*

    A combination should be considered so consumers can inform themselves and, ideally, understand what a smart device is basing the labelling on.

18. *Is there likely to be sufficient industry uptake of a voluntary label for smart devices? Why or why not?*
    a. If so, which existing labelling scheme should Australia seek to follow?

    If it is voluntary, uptake can be expected to be low unless there are incentives offered. We are unsure that consumer behaviour alone will be enough of an incentive.

    The CSA Singapore 4 Level labelling scheme provides a nice model but what it means may be opaque to consumers.

19. *Would a security expiry date label be most appropriate for a mandatory labelling scheme for smart devices? Why or why not?*

    Expiry labels may not align with expected support life of smart devices. Vendors

Global Headquarters 201 Mission St, Suite 2900 San Francisco, CA 94105 +1 415-599-1100

may also extend support life and thus an expiry label may not accurately represent the actual status.

Online “labels” may be another approach to consider. This could allow for more dynamic management of a “security expiry date” as device software gets updated.

20. *Should a mandatory labelling scheme cover mobile phones, as well as other smart devices? Why or why not?*

    It should. In our view mobile phones, with their frequent software updates, could leverage existing infrastructure to provide an electronic form of such a label. As mobile phones are core to our digital lifestyle and used for critical services such as banking, health and payments it is important that a user is made aware of if a mobile phone can get security related updates or not.

21. *Would it be beneficial for manufacturers to label smart devices both digitally and physically? Why or why not?*

    For reasons given earlier a digital labelling approach may be preferred. This would allow for devices to have their digital label presented on online management portals etc. This is important for small physical devices as well as for devices that may be installed in areas not readily accessible.

Chapter 8: Responsible disclosure policies

22. *Would voluntary guidance encourage Australian businesses to implement responsible disclosure policies? If not, what alternative approaches should be considered?*

    Intentionally left blank.

Chapter 9: Health checks for small businesses

Global Headquarters 201 Mission St, Suite 2900 San Francisco, CA 94105 +1 415-599-1100

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?*

    Yes, we believe tools and support for small business will have a positive impact on Australia's cyber security capabilities and readiness to deal with incidents.

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?*

    Intentionally left blank.

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

    Ensure that it is easily made available and supported so that small businesses can use it themselves or leverage third party expertise. Such third parties should be subject to some form of accreditation or license.

Chapter 10: Clear legal remedies for consumers

26. What issues have arisen to demonstrate any gaps in the Australian Consumer Law in terms of its application to digital products and cyber security risk?

    Intentionally left blank.

27. Are the reforms already being considered to protect consumers online through the Privacy Act 1988 and the Australian Consumer Law sufficient for cyber security? What other action should the Government consider, if any?

    Intentionally left blank

Global Headquarters 201 Mission St, Suite 2900 San Francisco, CA 94105 +1 415-599-1100

Chapter 11: Other issues

28. What other policies should we consider to set clear minimum cyber security expectations, increase transparency and disclosure, and protect the rights consumers?

    Intentionally left blank.

Global Headquarters 201 Mission St, Suite 2900 San Francisco, CA 94105 +1 415-599-1100