Executive Summary

The Medical Software Industry Association Ltd (MSIA) represents the interests of health software companies which power better outcomes for all Australians.

Our members include large international corporations operating in Australia as well as small start-up companies. MSIA members software is used by private, public, and not-for-profit providers. It includes systems used in hospital specialist, aged care, indigenous, disabilities, allied, research, primary care and preventative care settings. Virtually all health information in Australia is collected, communicated and managed by our members software.

The Medical Software Industry Association (MSIA) is Australia's leading industry body for providers of health software and a powerful force for innovation, productivity and better health outcomes for all Australians. Our members cover the digital management of Australians' healthcare from birth to death. Consequently, security and privacy are in the DNA of these companies which have an extraordinary record over the past decades.

The MSIA has been seeking[1]a harmonised data management framework, including privacy and security, together with other international healthcare organisations.[2]We are pleased that the Department is making clear progress in this regard particularly given the statistic of 11% which is touted as the percentage of Australian companies with the requisite digital readiness to manage cyber threats.[3] This, together with the ranking of healthcare as the 3rd highest target after Commonwealth and Jurisdictional Governments[4] (with which our member companies interact daily) makes this consultation of the utmost importance to our member companies.-

Our concerns are to ensure:

1. A balanced and contextual approach - To ensure that the level of security is effective and adequate but calibrated to match the circumstances in which the software is used. In other words, to get the right balance between a good UX, cost, benefit, and risk. Harmonisation with international standards, and standards within the Commonwealth and Jurisdictions is critical.
2. Realistic timing – Each organisation has its challenges, but all health software companies are currently under work force shortage pressures internationally. This must be acknowledged in the time periods and enforcement of these timetables
3. Development cost- The cost of additional security measures required for Government infrastructure is not always Business as Usual. The cost of the development is the same for large and small companies which raises equity issues. Furthermore, innovation and

[1] https://www.msia.com.au/public/137/files/MSIA%20Budget%20submission%20–%2027012023%20v2.pdf

[2]https://www.govinfosecurity.com/healthcare-leaders-call-for-cybersecurity-standards-a-21458

[3] https://itwire.com/business-it-news/security/only-11-of-companies-in-australia-are-ready-to-defend-against-cybersecurity-threats.html

[4] https://www.afr.com/technology/why-australia-is-such-a-juicy-target-for-cybercriminals-20230404-p5cxvn

productivity could be jeopardised if there is not assistance provided to health software organisations.

1. What ideas would you like to see included in the Strategy to make Australia the most cyber security nation in the world by 2020?

    - Consistency of regulation with other comparable nations in the regulations to enable certainty and scalability of health software. It would be excellent to be the most cyber safe nation in the world, but not if that means excessive security protocols out of step with the risks.

    - Extensive consumer education to assist consumers to comprehend the true value of cyber security and the correlating cost. It is difficult to compete otherwise with less secure and cheaper systems. In other words, help industry to demonstrate the business case for cyber security. The Minister's statement that *"Everyone has skin in the game when it comes to Australia's cyber security."* [5]Is so true, but ensuring that our population understands why will be the key to making this work. We are only as strong as our weakest link.

    - Harmonisation between the Commonwealth and Jurisdictional security regulations – adherence to 9 different sets of regulations inhibits innovation in security and more generally. Currently there are several consultations running in respect of security profiles for MyHR and other health software through the Australian Digital Health Agency ("ADHA") and the Department of Health and Ageing ("DoHAC"). This leads to additional cost and uncertainty with no apparent benefit when the current consultation together with the review of the privacy Act 1988 by the Attorney- General's Department will be likely to supersede them all.

    - Appropriate funding for organisations to ensure that smaller organisations are not inadvertently compromised.

    - A fit for purpose regime that reflects the risk through the response – in other words getting the balance right and adapting it in a well -understood manner.

2. What legislative or regulatory reforms should Government pursue to: enhance cyber resilience across the digital economy?
    (a) What is the appropriate mechanism for reforms to improve mandatory operational cyber security standards across the economy (e.g., legislation, regulation, or further regulatory guidance)?

[5] P.16 https://www.homeaffairs.gov.au/reports-and-pubs/files/2023-2030_australian_cyber_security_strategy_discussion_paper.pdf

- A harmonised National regulatory regime would be welcome provided it displays consistency with international best practice.

- Ultimately following regulatory guidance and transition time the certainty afforded by National legislation is likely to be most effective.

- Close and ongoing consultation with industry will be essential to monitor the regulatory burden versus the benefit.

- Extensions to the *Security of Critical Infrastructure Act* if deemed necessary will need to consider the ecosystem nature of industries like healthcare to ensure it is workable and does not have unintended safety risks.[6]

3. How should Australia better contribute to international standards-setting processes in relation to cyber security, and shape laws, norms and standards that uphold responsible state behaviour in cyber space?

- In the health software sphere, there are a number of technical organisations such as the Standards Development Organisations which have excellent capability and understanding of specific industry requirements. Working with such organisations will ensure Australia does not attempt to reinvent the wheel and is abreast of the existing complex regimes.
- The relationships which regulators like the TGA have with their international counterparts is another area which could be usefully leveraged in respect of security.

4. How can Commonwealth Government departments and agencies better demonstrate and deliver cyber security best practice and serve as a model for other entities?

- Consistency of approaches within and between Departments and Agencies would be an excellent starting point. For instance, even having a clear identification and authentication system with clear authority from a trusted Government source would improve the security posture for industry.

- Currently that is not the case which leads to cynicism and uncertainty in industry.

5. What can government do to improve information sharing with industry on cyber threats?

- Using the technique which the Department of Health and Ageing has adopted with its health Tech Talks would be welcome. It is an open forum where trust has developed to enable otherwise unheard of progress.

6. Should government consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators?

[6] https://www.msia.com.au/public/137/files/Submissions%20and%20Letters/MSIA-Critical-Infrastructure-Security-Submission_160920_ejh_asd_.pdf

- Any harmonisation is welcome.

7. How can government and industry work to improve cyber security best practice knowledge and behaviours, and support victims of cybercrime?
   a. What assistance do small businesses need from government to manage their cyber security risks to keep their data and their customers' data safe?

- Ongoing education of all Australians will have a positive effect on cyber security best practice and victims of cybercrime. The kinds of national education programmes which have worked in the past in respect of seat belts and .05 alcohol and driving should be considered in respect of this new risk to Australians.

- Small business cannot absorb the massive and ongoing costs of "going it alone" here. It is an area where Government assistance will be essential and expected.

8. How should we approach future proofing for cyber security technologies out to 2030?

   - See above.
   - Once a clear framework is settled it will need to be constantly evolving so ongoing engagement with industry will be key to ensuring a balanced approach for software development.

9. Are there opportunities for government to better use procurement as a lever to support and encourage the Australian cyber security ecosystem and ensure that there is a viable path to market for Australian cyber security firms?

   - Yes. See above.

   - Having templates for procurement which are nationally accepted both in public and private procurement would have enormous efficiency and productivity gains. The Attorney-General's Department has suggested privacy notice templates in its consultation on the *Privacy Act 1988.*

   - A similar approach would be excellent if deployed for security. Not only would it increase the understanding amongst industry and the marketplace through having one and not multiple regimes, but it would mean that industry could focus on hardening its posture rather than having a diverse range of bespoke approaches for all the various procurements.

10. How should the Strategy evolve to address the cyber security of emerging technologies and promote security by design in new technologies?

- Having a clear overarching and outcomes-based framework which is principles based and not prescriptive will facilitate security by design the way it has enabled privacy by design in some areas.

- Once there is clarity, security services can be commoditised enabling greater concentration of resources on emerging threats.

Timing

Many health software companies are currently uplifting their products following several years of intense unplanned development in response to urgent government policy priorities during the COVID-19 Pandemic. Work like the Services Australia, Adaptors to Web Services, uploads to the Australian Immunisation Register and patients immunisations bookings and virtual care were done often without financial reward,. These were all a part of the Government agenda. It was well beyond the business-as-usual work required to interact with Government. All companies require the same effort, large and small, to effect the proposed security uptake. Consequently, to avoid unintended consequences on competition and innovation, where Government can provide the highest standard gateways to support security and harmonisation noted above, this will alleviate some of the significant impost and inequity.

Our industry like other tech sectors simply lacks the number of qualified people to do the required work right now. The workforce issue is severe and not of anyone's making. Any proposed timetable needs to be cognisant of this limitation.

Development and Testing Cost

As noted above, industry has contributed to the national health cause since 2019 during the Bushfires, right through COVID-19. It is now under pressure to deliver on some of the customer driven roadmap to keep the industry competitive with international industry. The legal requirements likely as a result of this consultation, and that by the Attorney General's office and will have their own timetables and nuances.

It is critical that where possible industry is supported with resources for development and consumer education. And implementation. Without this, the best and most secure software in the world will have little if any impact.

Conclusion

Despite the demands on the health software industry recently, it's scorecard in security has been exceptionally high. Their knowledge of the customer base together with a high level of support and education and expert implementation could be used as an exemplar for the uplift in security in our sector which arguably manages the most sensitive and valuable information of all Australians.

The MSIA welcomes any queries or other interactions from the Department, and look forward to strengthening Australia's security in the health software sector.

Emma Hossack

CEO MSIA

15 April 2023