2023-2030 Australian Cyber Security Strategy - Discussion Paper

Mariam Sleiman

15 April, 2023

Cyber Security Strategy Discussion Paper Questions

Abstract

I’ll discuss some strategies that can help the Australian Government in order to see Australia the most secure country in 2030. I’m going to answer all the questions from a cyber security specialist perspective

1. **What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?**

I think that most of the cybercrimes in Australia have been happening because of the low consciousness of citizens to use the internet safely, so the importance of spreading awareness about cyber security on media, through cooperating with other government sectors such as the educational and media industry, specifically most users who fall in the trap are teenagers. It plays a big role in evolving Australia's digital security.

2. **What legislative or regulatory reforms should Government pursue to: enhance cyber resilience across the digital economy?**

- Governments can require businesses to report cyber incidents to a central authority
- Governments can incentivize or mandate that businesses purchase cyber insurance to protect against financial losses resulting from cyber incidents
- Governments can mandate that businesses comply with specific cybersecurity standards to ensure that they have adequate protections against cyber threats
- Impose laws that require businesses to protect sensitive customer data and provide disclosure in the event of a data breach.

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)?

Imposing strict laws and fines concerning the cyber crimes can be one of the appropriate mechanism, such as those who do scamming, blackmailing and other digital crimes should be pursued by the police and sentence them.

Industry Standards: These standards can be developed by industry associations or standard-setting bodies and can be used by organizations to ensure they are meeting minimum cybersecurity requirements.

Improve collaboration between industry and government. This can include information sharing initiatives, joint cybersecurity exercises, and other programs that promote collaboration and partnerships

b. Is further reform to the Security of Critical Infrastructure Act required? Should this extend beyond the existing definitions of 'critical assets' so that customer data and 'systems' are included in this definition?

As we know if there is any threat on the infrastructure it will lead to a massive chaos and hinder the public transports. For example, if an attack happened on Uber or any other transport, plus, if we are not taking any cautious or prediction for this kind of attack to happen, or have at least a clear strategy

It will help both the customers and government to prevent this kind of attach to happen as much as possible, and to have some specific methods to know who

was behind the attack, what the cause was, what it affects and what we should do after the attack.

Also investing in critical infrastructure security and it can include funding research and development of new technologies and tools

c. Should the obligations of company directors specifically address cyber security risks and consequences?

Sure, most companies don't care about their data security and take the essential security standards until an incident happen then they will start to hire cyber security specialists.

They lack the awareness for their employees, the transactions and the shared data with other companies which have a weak secure system, that result to data leakage and other catastrophe incidents.

d. Should Australia consider a Cyber Security Act, and what should this include?

I think it would be a great decision if Australia adapts a Cyber Security Act, as it will indicate that Cyber security is a serious aspect in Australia and it will prevent much more attacks from happening as it will reflect to other countries about how Australia is evolving with the rapid pace of technology. This can include several points such as:

· Any type of social engineering attack on companies, government sectors, should be grounded because sensitive information that has a direct access to countries

(makes social engineering not an easy method for attacking those sensitive as most hackers attack successfully through social engineering, despite people's awareness, so it can be a good point to prevent people from doing social engineering attack.

· Supporting security specialists to encourage them work effectively by rewarding them prizes, money…

· Provide law enforcement, other security organizations with the tools they need to investigate and prosecute, take their report or opinions into consideration.

· Incident response procedures

· Monitoring the Dark Web users and the illegal stuff that’s being included in Australia

· Restrict spying methods:

· Opening some bug bounty programs or cyber challenges to encourage those who are enthusiasts and who have the skills to attract them and put their skills in the right place.

e. How should Government seek to monitor the regulatory burden on businesses as a result of legal obligations to cybersecurity, and are there opportunities to streamline existing regulatory frameworks?

Monitoring the regulatory burden on businesses as a result of legal obligations to cybersecurity requires a proactive and collaborative approach between governments and businesses. It can provide guidance for business on how to comply with regulations including best practices, tools, resources, and researchers. Although it can conduct surveys and see the reviews of other regulations and receive feedback from stakeholders to see where regulations can be consolidated.

f. Should the Government prohibit the payment of ransoms and extortion demands by cyber criminals by: (a) victims of cybercrime; and/or (b) insurers? If so, under what circumstances?

Victims of cybercrime may feel that they have no other choice but to pay the ransom in order to regain access to their data or systems. Prohibiting the payment of ransoms may also result in increased costs for businesses and insurers, as they may need to invest in additional cybersecurity measures to prevent cyberattacks or to recover. If the government were to prohibit the payment of ransoms and extortion demands, it would need to carefully consider the circumstances under which such a prohibition would apply. For instance, if it's related to certain terrorist groups or countries and other political issues.

From my point of view, it would be better if the government prohibit the payment of ransoms and extortion demands by cyber criminals by victims of cybercrime, because it may be easier to spot the attacker if he knows that a normal citizen is going to be attacked rather than the insurers, he would not gather anymore because of their actions are profitable

i. What impact would a strict prohibition of payment of ransoms and extortion demands by cyber criminals have on victims of cybercrimes companies insurers

It would be much safer for the victims as it's not causing them to be in any sort of touch with the criminals so they don't feel intimidated, but the issue is that the insurers as they may face increased costs associated with covering losses resulting from cyberattacks. Without the ability to pay ransoms, insurers may need to pay out higher claims to cover the costs of remediation efforts or lost data. Even companies, it would cause them to increase costs in order to respond to it.

While It will provide a safe tech environment for the users to have strict prohibition of payment of ransoms, it will make the attackers to not try so hard to attack the victim for profit and at the same time, but at the same time:

- It will increase the anonymity of attacker which hardens the process of getting to prosecute him
- The companies might suffer from low trust if any data leakage happens
- It will increase the financial losses as it may disrupt some services.

· If the attacker has access to a sensitive place where he can access most stakeholders' sensitive data, he may have the access to their own machines or digital devices, which will expand the extortion

It can cause a bad reputation if they can't have any profit that can make them post anything they get.

g. Should Government clarify its position with respect to payment or non-payment of ransoms by companies, and the circumstances in which this may constitute a breach of Australian law?

The government should clarify its position with respect to both by companies,
With respect to payment: the government should provide guidance and clarity on the legality of paying ransoms, as well as the potential circumstances in doing so .
With respect to non-payment: the government should help or save the victim by knowing the root cause of ransom, who was behind it and all the exclusive information.
With paying or non-paying, the decision ultimately lies with the company, but the government could make it easier for them to take the right choice and reduce the prevalence of ransoms

Moreover, the payment or non-payment ransoms by companies should be under circumstances and not breaking the Australian law such as the regulations, specific standards.

And it depends on the company, its category or industry-specific, specifically it's related to health or governmental services.

3. How can Australia, working with our neighbors, build our regional cyber resilience and better respond to cyber incidents?

By cooperating with other cyber companies and governments security sectors, to put a strategy that serves the same values for both, taking other cyber security specialist experts' opinions or discussions about any incident.

Doing international cyber conferences that could attend it the greatest minds of cyber experts national and international to highlight some of the best strategies and methods that should be taken to secure our country.

4. What opportunities exist for Australia to elevate its existing international bilateral and multilateral partnerships from a cyber security perspective?

Such great opportunities and Australia is going to witness a cyber revolution if it takes the decision to have partnerships with other countries as new methods can be exchanged, more secure devices, more cautions and learning the lessons from other countries if any attack happen. Most importantly, if there is any incident that happens in Australia, other countries could help, as it will take less time and more efficient to reduce cyber crimes.

5. **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?**

Australia might improve the international standards-setting processes in cyberspace through maintaining a great strategy involving experts advices, governments guide, to monitor digital devices, by doing a lot of research, funding research, encouraging the cyber enthusiasts to enter the filed in Australia and giving them reward, enhancing the cyber security field.

When Australia is being one of the most secure countries, and the best nation worldwide that has the strongest strategies, it could help the international standards by imposing certain laws, amalgamating cyber companies to get a project together, giving new methods and advices

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

When the government departments collaborate with other entities, such as private sector organizations, to share information and best practices and to develop coordinated approaches to cyber security . monitor their systems and networks for potential threats and vulnerabilities, and conduct regular testing to ensure that their security measures are effective. They can deliver best practice by caring about the cyber security practices, standards, measures, learn from past incidents, doing sessions together, collaborating with each other to spread awareness in the media, educating people about the importance of cybersecurity and its latest technology.

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

· Provide incentives for information sharing: The government can provide incentives for industry partners to share threat intelligence, such as tax breaks, grants, or other financial incentives. This can help to encourage greater participation in information sharing programs and promote a culture of collaboration and shared responsibility..

· Have a shared platform to discuss threats, the new discovered viruses, new tools used, vulnerabilities for all Australians, a specific platform for Australia.cyber security

8. **During a cyber incident, would an explicit obligation of confidentiality upon the Australian Signals Directorate (ASD) Australian Cyber Security Centre (ACSC) improve engagement with organisations that experience a cyber incident so as to allow information to be shared between the organisation and ASD/ACSC without the concern that this will be shared with regulators?**

   It’s totally fine to share the information with the regulators as it will provide a faster, more secure solution than the organization itself, as it will help to have more ideas and discussions. In the end, we try to get out of the incident with as low cost and damage as we can .

9. **Would expanding the existing regime for notification of cyber security incidents (e.g. to require mandatory reporting of ransomware or extortion demands) improve the public understanding of the nature and scale of ransomware and extortion as a cybercrime type?**

Well, it can help to understand more the scale of ransomware and taking precautions to protect, but that doesn’t mean it will end the ransoms or cybercrime as some people might not have the knowledge of knowing the security strategies while it can benefit the bad guy to have more ideas to expand their unethical doing.

10. **What best practice models are available for automated threat-blocking at scale?**

We can use AI-ML algorithms models to make an automated threat-blocking that can contain all the threats types such as:

Web application security threats example XSS, SQL injection, Denial of service

Hijacking type, bypassing authentication,

- Doing an automated application that searches for a virus, detect its type, fix it

- Make an AI tool that searches for certain vulnerabilities on government websites, public sectors such as hospitals, infrastructure related,

- How?

There are several methods the Australian Government can take to make automated models :

First, having a team consists of cyber security experts or AI to do automated tools

Secondly, giving opportunities to international cyber security experts as it will thrive Australian and at the same time international people may experience the best

Doing competitions locally, internationally to get more ideas, strategies

Some models:

1. Writing a code contains AI algorithms, putting specific algorithms to search for example any document, application, link, even it can be physical devices like USB to detect any virus

2. Checking the websites or links to know if there are any hidden redirects

3. All types of phishing attack can be spotted with threat-blocking tools

11. Does Australia require a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda?

Cyber skills requires more specialized that goes beyond STEM such as providing opportunities, internships, job-training. Although, it needs regulatory compliance, risk management, network security, cryptography…

Cyber threats are constantly evolving, and the skills needed to address them must also evolve. A tailored approach to cyber skills development can help ensure that the workforce has the latest knowledge and skills needed to combat emerging threats.

12. What more can Government do to support Australia's cyber security workforce through education, immigration, and accreditation?

The government has an ultimate role in evolving Australia's cyber security strategy,

It can cooperate with the educational sector, providing campaigns for the students on preaching them what the possible threats they may face, how to face them in a wise way, also, it can be through documentaries, and for the immigration part, facilitating the visa for the cyber security professionals and specially to attend international conferences that are located in Australia, it may attracts the world's most professional cyber security expert and make Australia a cyber security nation. Also, collaborating with different business with the local business and universities, to spot the talented security researches.

Governments can provide financial support for foreign cyber security professionals to obtain accreditation in their country. This will make it easier for them to integrate into the local job market and contribute to the local cyber security industry.

accreditation standards from other countries. This will enable foreign cyber security professionals to easily demonstrate their qualifications and credentials in the local job market.

13. How should the government respond to major cyber incidents (beyond existing law enforcement and operational responses) to protect Australians?

First, when an incident happens, the government should make it clear, what and how it has happened, the potential impact, and what actions to take to secure ourselves to not fall into it.

Secondly, maintain an investigation, its scope, source and impact and develop strategies to prevent it in the future.

Developing a plan involves the different roles of agencies, the protocols and the procedures for incident response for each one, using a specific framework can help this.

Provide financial assistance to recover after the incident

Strengthen security regulations and standards

Implementing mandatory reporting requirements, imposing penalties on the attackers, providing incentives for organizations.

Having awards, ceremony, bub bounty platform, hall of fame to encourage security researches and even hackers to not to the offending way instead they can use it for the goodness and in helping the organizations after they feel comfortable with the government and trust it, I believe that it will reduce the cyber criminals.

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

Having a single platform for Australian incidents report can be a great idea, as it will have consistent reporting standards, scope, policy, the required essential awareness and it will enhance the collaboration of organizations

14. What would an effective post-incident review and consequence management model with industry involve?

1. Responding quickly and effectively through asking experts, identifying scope, expect the damage severity and to restore operations. Backup of information if possible
2. After this, we should have a review and report for identifying the type of attack, its impact, its coincidences on citizens
3. Identifying how that happened, improve the areas that were in the possible cause of the threat and taking more secure standards to enhance the overall organization security
4. Communication and reporting it to the public if possible, preach the citizens how these attacks could happen, how they can protect themselves, what kind of seps they should take

15. How can government and industry work to improve cyber security best practice knowledge and behaviors, and support victims of cybercrime?

- Education: educate the young generation ot have a secure Australian generation, knowing the importance of being secure digitally

- Sharing the information on a special platform : any kind og bugs were found, threats has happened, damages, possible threats that could take place…
- Collaboration with international cyber organizations or agencies
- Supporting the local cyber businesses to improve and grow as it may have the chance to defeat or beat the international cyber organizations by having strong strategies or more secure technologies
- Having laws that supports the victim and protect him to feel in peace that the attacker won't have any touch with the victim or make his life in danger

a. What assistance do small businesses need from government to manage their cyber security risks to keep their data and their customers' data safe?

- Funding and Grants .Small businesses may need financial assistance to invest in cybersecurity technologies and services. The government can offer funding and grants to support cybersecurity initiatives, particularly for businesses in sectors that are critical to national infrastructure.
- Technical assistance and support
- Providing free advices and consultations from experts of the field
- Cooperation with the big businesses

- Checking them up regularly to monitor the status of their job, if it’s going good and the business is growing bigger or if it needs any help.

16. What opportunities are available for government to enhance Australia’s cyber security technologies ecosystem and support the uptake of cyber security services and technologies in Australia?

· International collaboration

· Promoting education

· Focusing on the infrastructure security as it is related to the government issues, it can be like funding certain researches

· Encouraging the startups of cyber security business, which will make entrepreneurs to develop more and test new ideas and technologies, as it will create a vibrant cyber security ecosystem

·Insurance incentives

·Providing emergency response services.

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

· Strengthening authentication

· Inventing new AI models related to security, threat-blocking, detecting vulnerabilities, stronger password, stronger websites.

· Cloud based data, implement security strategies to secure it more

18. 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?

setting cybersecurity standards and requirements for the products and services they purchase

support cybersecurity startups and emerging firms by providing them with opportunities to compete for government contracts.

Offer incentives for innovation

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

Now there a lot of physical attacking, such as the public charger cable that can steal the oneself sensitive information,

Cybersecurity should be integrated into the design process of new technologies. Security features such as authentication, access control, encryption, and monitoring should be implemented at the earliest stages of development.

Regular updates and maintenance

20. How should government measure its impact in uplifting national cyber resilience?

National Cybersecurity Strategies

Cyber Resilience Index: Governments can develop a Cyber Resilience Index that measures the level of cyber resilience across different sectors and industries in the country. This index can help identify areas where resilience needs to be strengthened and track progress over time.

surveys and other assessment methods that evaluate the level of knowledge and adherence to cybersecurity best practices.

21. What evaluation measures would support ongoing public transparency and input regarding the implementation of the Strategy?

- Sharing information publicly on threats, its impact, how it did happened, to prevent attacks the same type
- Public consultation and international cooperating
- Regular reports and statistics
- Metrics and Key Performance Indicators (KPIs): The Strategy should include clear and measurable metrics and KPIs that can be used to evaluate progress and report back to the public. These metrics should be easily understandable by the public and should track the effectiveness of the Strategy.