
# NATIONAL AUSTRALIA BANK SUBMISSION

## Australia's 2020 Cyber Security Strategy

4 November 2019

## Executive Summary

National Australia Bank (NAB) welcomes the opportunity to provide a submission to the Department of Home Affairs relating to its Discussion Paper on Australia's 2020 Cyber Security Strategy. The Strategy development comes at a time when cyber threats are becoming increasingly prevalent and significant. NAB thanks the Department of Home Affairs for accepting this submission.

Whilst cyber security is a shared responsibility, the Government inevitably has, and must take, a leadership role, in partnership with the private sector, to advance cyber security in Australia.

Below, NAB has provided key overarching views in relation to the Discussion Paper. Responses to each of the 26 questions posed within the Discussion Paper are included in the Appendix.

### The Role of the Government

NAB agrees that the Government plays an integral role in addressing cyber threats, however change is required. The Government has the opportunity to take a more offensive and disruptive approach, through greater regulatory influence and enforcement. The Government should also leverage partnerships with the private sector to tackle threats on a national level.

Whilst we focus on and enhance the cyber security capability of the Government agencies and the private sector, it is important that the Government does not forget individuals, small businesses and not-for-profit organisations which often lack the knowledge, skills or finances to protect themselves from cyber attacks. The Government should foster a risk awareness culture to protect the public and the economy. This includes providing active support to prevent, monitor, detect and respond to cyber-attacks.

As per the Australia's 2020 Cyber Security Strategy Discussion Paper, $2.3 billion was stolen from consumers in 2017. $2.1 billion per year, at least, is the estimated impact of identity crime in Australia. 80% of known victims reported a psychological impact. Addressing these issues would result in economic and social benefits.

### Priorities

As a priority, the Government should focus on threats and actors that target critical and systemic government network infrastructure. It should also provide support against threats to critical infrastructure such as finance, utilities and health to ensure operational resilience for these critical economic functions.

The Government should consider developing a national and international accreditation system for digital goods and services, providing minimum security standards to enhance consumer confidence; and consider a public rating framework for global and local businesses based on compliance with minimum standards.

To minimise loss, the Government should consider partnering with industry and Internet Service Providers to set mandatory minimum requirements for hardware, operating systems, auto-patching and the installation of anti-virus, malware, ransomware tools, as well as the introduction of strong regulations around controls such as encryption, patching and penetration testing.

**Funding**

NAB recommends the Government reviews the amount of funding dedicated to implementing any Cyber Strategy. Spend on Cyber Security must be seen as an investment and must be commensurate with the quickly changing landscape. Both the Government and the private sector must bear that cost.

Comparisons of the Government spend on cyber security are included below.

- *Australia*: The Cyber Security Strategy includes investments of more than $230 million for the period 2016-2020. (Source: Department of Industry, Innovation and Science, Australian Government)
- *United Kingdom*: The current National Cyber Security Strategy runs from 2016 to 2021. It has a 1.9 billion pound budget. (Source: UK Parliament Publications)
- *United States* : TheFY2019 budget includes $15 billion for cyber security related activities, a $583.4 million (4.1%) increase above the FY2018 estimate. (Source: Cyber Security Funding – The White House)
- *Canada*: 2018 budget, provided for substantial investments in cyber security totalling more than $500 million dollars over five years. (Source: Public Safety, Canada Government)

**Creation of the National Advisory Council**

Similar to MAS Cyber Security Advisory Panel (CNAP) which comprises cyber security experts and thought leaders, NAB recommends the creation of the National Advisory Council for Cyber Security which is an important and necessary initiative to effectively tackle cyber threats. It will enable better cooperation between the government and the private sector. Both sides can learn from each other and benefit through the legislative power of the Government and the financial power of some key players of the private sector. However, the goal needs to be for the benefit of the public and the economy and for it to be successful, it is essential that it sets strategic and clear objectives which are in alignment with ever-changing cyber landscape and there is an appropriate representation from both the Government and the private sector.

NAB would be pleased to discuss its abovementioned views, or any of its responses to the 26 individual questions, which are contained within the appendix.

## Appendix: NAB responses to individual questions posed within the Discussion Paper

1. **What is your view of the cyber threat environment? What threats should the Government be focusing on?**

   The cyber threat environment is dynamic, increasing and expanding. Financial institutions have often been the target of such attacks, but attacks on other industries are becoming increasingly common. Attacks on critical services such as utilities, emergency services, health services, domestic and industry Internet of Things devices such as Supervisory Control and Data Acquisition systems (SCADA) are becoming more frequent

   As a priority, the Government should focus on threats and actors which target critical and systemic government network infrastructure. It should also provide support against threats to critical infrastructure such as finance, utilities and health to ensure operational resilience for these critical economic functions.

   Other potential focus areas include:

   - Increases in guidance or regulatory oversight, including Subject Matter Experts;
   - Establishment of eCommerce minimum standards;
   - Review of Supply chain risk and raising the bar on suppliers involved in government procurement channels;
   - Controlling the reach of state actors and criminal organisations;
   - Addressing Internet of Things related threats as more and more devices are connected to the internet;
   - Addressing threats affecting organisations which have a culture of openness and collaboration, for example universities and schools; and
   - Public education and awareness campaigns, such as phishing and scam education, the use of anti-virus, malware, ransomware and password manager tools, and the promotion of existing campaigns such as StaySmartOnlineWeek and Alert Service.

2. **Do you agree with our understanding of who is responsible for managing cyber risks in the economy?**

   NAB agrees that Government, businesses and individuals share responsibility for cyber security.

3. **Do you think the way these responsibilities are currently allocated is right? What changes should we consider?**

   The Government can and must provide active support through partnerships with private organisations to tackle threats effectively on a national level. The Government must also become more disruptive and offensive through legislative changes. Conventional security approach with reactive measures may no longer be sufficient as attacks become more sophisticated.

   Cyber risk management should become more prevalent across all economic sectors. Industry has a critical role in this regard. Industry and large businesses should shoulder more accountability to raise awareness regarding cyber threats

amongst their customers. They should also ensure that their cyber defence capabilities are continually enhanced in alignment with changing cyber landscape. For individuals and small businesses, the Government should play a larger role in fostering the risk awareness culture to protect the public and the economy, and partner with business to do so. This includes providing active support to individuals and small businesses to prevent, monitor, detect and respond to cyber-attacks.

4. **What role should Government play in addressing the most serious threats to institutions and businesses located in Australia?**

The Government should:

- Extend existing partnerships with financial institutions and other large corporations to improve the provision of national security data on threat types and attack means;
- Partner with industry and Internet Service Providers to set mandatory minimum requirements for hardware, operating systems, auto-patching, the installation of anti-virus, malware, and ransomware tools, as well as assist public compliance through subsidies and hardware buy-back programs;
- Provide timely notification of vulnerabilities;
- Ensure timely and effective coordination amongst state and federal law enforcement agencies;
- Increase penalties and enforcement for those who commit cyber-crime;
- Fully assess and embed cyber security into open banking regulations before they are implemented;
- Continue to work actively with the international community, governments and other agencies to prosecute cyber criminals around the world, especially in areas typically outside the reach of law enforcement, for example: Ukraine, North Korea, Russia, Iran and many African countries. This should be multi-faceted and include support of sanctions where necessary;
- Improve education and awareness, especially for end-users such as individuals, small businesses and not-for-profit organisations;
- Provide active support and guidance to individuals, small businesses and not-for-profit organisations to prevent, monitor, detect and respond to cyber-attacks; and
- Encourage cyber study, for example by removing HECS fees from territory courses or subsidising these areas of study.

The Government has the opportunity to play an active role in assisting large businesses to drive agendas of national interest for the benefit of customers and the general public.

5. **How can the Government maintain trust from the Australian community when using its cyber security capabilities?**

To maintain trust from the Australian community, the Government must continue to materially improve its threat posture and intelligence gathering, including border related controls for all entries into the Australian computer network. Additionally, the Government should:

- Prioritise its efforts and promoting the activities it undertakes, as well as the results;
- Build its capability to maintain and protect core foundations and critical infrastructure;
- Provide strong protocols that allow cyber threat data to be collected and shared widely without revealing sources; and
- Be transparent about how all data that the Government accesses is used and disposed of;
- Ensure Government agencies promote best practice cyber security practices, for example by following the essential eight, avoiding the utilisation of live URLs in emails to constituents, and utilising DMARC (Domain-based Message Authentication, Reporting and Conformance);
- Set goals for the cyber preparedness of its own agencies, including high NIST CSF (National Institute of Standards and Technology Cyber Security Framework) levels as expected for a nation state; and
- Ensure investigations and actions are strictly policed and reported openly.

6. **What customer protections should apply to the security of cyber goods and services?**

   In supplying cyber goods and services, NAB suggests:

   - Consumer protections should apply in relation to the provision of all cyber goods and services, including Internet of Things devices;
   - Every cyber good should be capable of being patched and having its default password changed;
   - Robust payment methods with inbuilt fraud controls should exist for the purchasing process, and that regulation to address instances where protection is not provided should be in place;
   - The development of a national and international accreditation system providing minimum security standards to enhance consumer confidence; and
   - Consideration of a public rating framework for global and local businesses, based on compliance with minimum standards.

7. **What role can Government and industry play in supporting the cyber security of consumers?**

   The Government and industry can support the cyber security of consumers by:

   - Providing advice and guidance wherever possible;
   - Providing additional education and leadership;
   - Spreading awareness via trusted channels, including the delivery of baseline free protection services (e.g. eCommerce health checks);
   - Centralising cyber education platforms; there are currently eight government agencies conducting similar work around StaySmartOnline;
   - Developing a national and international accreditation system which would provide minimum security standards to enhance consumer confidence; and
   - Considering a public rating framework for global and local businesses, based on compliance with minimum standards.

8. **How can Government and industry sensibly increase the security, quality and effectiveness of cyber security and digital offerings?**

   The Government and industry can increase the security, quality and effectiveness of cyber security and digital offerings by:

   - Setting minimum standards across industries;
   - Introducing baseline security training through technology certifications;
   - Differentiating between poor technology management and poor security management with respect to security incidents;
   - Improving education, awareness, support and guidance to prevent, monitor, detect and respond to cyber attacks; particularly to end-users such as individuals, small businesses and not-for-profit organisations,
   - Partnering with consider partnering with industry and Internet Service Providers to set mandatory minimum requirements for hardware, operating systems, auto-patching and the installation of anti-virus, malware, ransomware tools, and assist with public compliance through subsidies;
   - Providing active support and guidance to individuals, small businesses and not-for-profit organisations
   - Offering solutions and services, to enable end-users to defend themselves;
   - Providing greater oversight of the private sector with respect to security and threat posture reporting;
   - Developing a national and international accreditation system which provides minimum security standards to enhance consumer confidence; and
   - Considering of a public rating framework for global and local businesses, based on compliance with minimum standards.

9. **Are there functions the Government currently performs that could be safely devolved to the private sector? What would the effect(s) be?**

   Established private sector participants could take a greater role in collecting data and conducting analysis of this to aid in cyber security measures. This involvement would need to be managed through appropriate frameworks and defined engagement conduits.

   The private sector should also be encouraged to share research into, and development of, cyber security technologies.

10. **Is the regulatory environment for cyber security appropriate? Why or why not?**

    Australia's regulatory environment is maturing. Other western countries are more advanced in relation to threat intelligence security testing such as Controlled, Bespoke Intelligence-led Cyber Security Testing (CBEST) in the United Kingdom, Threat Intelligence-based Ethical Red Teaming (TIBER) in the European Union and intelligence-led Cyber Attack Simulation Testing (iCAST) in Hong Kong.

    There is an opportunity for Australia to follow other countries and provide more directive legislation in relation to cyber security. The notion of Operational Resilience, which is broader than cyber security, is not yet present in Australia, but is immersed in the United Kingdom.

For the finance industry, CPS234 is emerging and has taken effect, however could be more prescriptive and further compel the use of industry good practice "essentials" such as encryption, patching, penetration testing. Countries such as Singapore and the United States could be looked to for best-practice examples.

NAB suggests that cyber security could be regulated by having multiple regulatory bodies for various industries, especially those which provide critical infrastructure and are government agencies, with consistent objectives (similar to APRA and CPS234 for financial institutions). Alternatively, there could be a regulatory body which exists solely to regulate Australia's cyber security environment with varying levels of standards based on the type of industry. The relevant powers, consequences of non-compliance, and effectiveness of consequences in deterring behaviour should also be reviewed. It is also important that any regulation does not stifle innovation.

NAB considers Australia's data privacy laws to be sufficient.

**11. What specific market incentives or regulatory changes should Government consider?**

The Government should consider:

- Increasing its powers to enable it to be more disruptive where it serves Australian entities or customers interest through change in legislation;
- Formalising national initiatives;
- Ensuring relevant capital reserves are available for cyber security-related issues;
- Establishing a regulatory body that mandates, reviews patching and testing, and enforces financial penalties, for example GDPR 8%; and
- Introducing penalties for failures to meet basic cyber security hygiene requirements.

**12. What needs to be done so that cyber security is 'built-in' to digital goods and services?**

To ensure cyber security is built in to digital goods and services, the Government should:

- Consider a public rating framework for global and local businesses, based on compliance with minimum standards;
- Introduce penalties for failures to meet basic cyber security hygiene requirements;
- Differentiate technology management issues and product issues and drive incentives for secure services and dis-incentives for insecure services;
- Monitor and act on supply-chain risks;
- Increase oversight on vendors, particularly those who hold Personal Identifiable Information, and hold them accountable; and
- Educate the public to consider security before procuring products.

13. **How could we approach instilling better trust in ICT supply chains?**

The Government should establish a national register of audited companies. This could reduce the costs of CPS234 compliance and could be modelled on SOC 2 or even related to compliance with the "Essential 8".

14. **How can Australian governments and private entities build a market of high-quality cyber security professionals in Australia?**

The Government and private entities can build a market of high-quality cyber security professionals by:

- Introducing early education on cyber security through school education which educate on the benefits of careers in cyber security;
- Partnering to develop curriculums with private and educational entities;
- Providing HECS-free or subsidised cyber security courses at universities to build talent pipeline. These could incorporate on-the-job training;
- Including cyber security qualifications on skilled migrant visa list;
- Introducing re-training programs for adults, especially veterans; and
- Introducing specialised courses aligned to industry focus areas and driven by industry objectives.

15. **Are there any barriers currently preventing the growth of the cyber insurance market in Australia? If so, how can they be addressed?**

Barriers to growth of the cyber insurance market include:

- Lack of transparency of the products and how they work;
- Lack of awareness of insurance products and their benefits; and
- Lack of skills and knowledge around cybersecurity-related risk and issues and how to quantify cyber-related losses.

Insurance policies could be broken down into specific cyber-related events that would be covered based on industry, likelihood of occurrence and consequences.

The Government could also consider a register of companies which have shown themselves to be compliant with the Essential 8, and work with insurance bodies to promote lower premiums for compliant organisations.

16. **How can high-volume, low-sophistication malicious activity targeting Australia be reduced?**

The Government must continue to materially improve its threat posture and intelligence gathering, including border related controls for all entries into the Australian computer network.

The Government should, continuously work to improve its mechanisms for detection, containment and blocking of sources of phishing and scams, through collaboration with private enterprises.

The Government should also set goals for the cyber preparedness of its own agencies, including high NIST CSF (National Institute of Standards and Technology Cyber Security Framework) levels as expected for a nation state.

17. **What changes can the Government make to create a hostile environment for malicious cyber actors?**

To deter malicious cyber actors, the Government should:

- Increase penalties for the organised crime organisations and individuals; and
- Lengthen jail terms.

18. **How can governments and private entities better proactively identify and remediate cyber risks on essential private networks?**

To proactively identify and remediate cyber risks on essential private networks, the Government can:

- Enhance joint initiatives and taskforces funded by both the Government and private entities;
- Incentivise private entities that can see the Indicator of Compromise's; for example: telecommunication companies to detect and report;
- As above, consider developing a register of companies which are compliant with the Essential 8 Framework, and work with insurance bodies to promo
- Introduce stronger regulation around controls such as encryption, patching and penetration testing.

19. **What should private networks be considered critical systems that need stronger cyber defences?**

The term "critical systems" should be defined. Similar to the US Homeland Security National Infrastructure Protection Plan, be it public or private, the definition should focus on the type instead of ownership. NAB views the following as being "critical systems":

- Chemical Sector
- Commercial Facilities Sector
- Communications Sector
- Critical Manufacturing Sector
- Dams Sector
- Defence Industrial Base Sector
- Emergency Services Sector
- Energy Sector
- Financial Services Sector
- Food and Agriculture Sector
- Government Facilities Sector
- Healthcare and Public Health Sector
- Information Technology Sector
- Nuclear Reactors, Materials, and Waste Sector
- Transportation Systems Sector
- Water and Wastewater Systems Sector

20. **What funding models should Government explore for any additional protections provided to the community?**

The Government should consider government grants, incentives and tax concessions for cyber safety-related matters. The awarding of grants, incentives or concessions should be based on, for example, industry certifications, accredited external audit reports.

The Government should also consider subsidising end-users such as individuals, small businesses and not-for-profit organisations meeting mandatory minimum standards.

Considerations for funding include:

- Commonwealth funding;
- Private sector funding, particularly through financial institutions, large telecommunication and technology companies;
- Financial penalties for digital goods and services providers which fail to meet basic cyber security hygiene requirements;
- Greater financial penalties for corporations which experience repeated data breaches or compromises and also for cyber criminals; and
- Potentially building publicly-owned businesses which become self-sufficient in meeting essential community protections and selling these as regulated service providers (akin to 'cyber-police' entities responsible only for detection and baseline protection).

21. **What are the constraints to information sharing between Government and industry on cyber threats and vulnerabilities?**

The potential for regulatory or political ramifications is a constraint to information sharing between the Government and industry.

If the Government penalises industry during the information process, this would be a deterrent.

22. **To what extent do you agree that a lack of cyber awareness drives poor consumer choices and/or market offerings?**

It is certainly true that in some cases, consumers lack awareness and make poor choices. Where consumers are aware of potential cyber risks and of the benefits and deficiencies of product offerings, they are able to make better choices. However, due to competing preferences, such as cost, consumers so often make poor choices regardless of awareness. In such instances, competition drives greater quality.

23. **How can an increased consumer focus on cyber security benefit Australian businesses that create secure cyber products?**

An increased consumer focus on cyber security would result in:

- Increase in sales of secure cyber products;
- Public respect; and

- An overall positive contribution towards the employment and the economy.

**24. What are examples of best practice behaviour change campaigns or measures? How did they achieve scale and how were they evaluated?**

Government bodies have run multiple campaigns to educate and change behaviours such as drink-driving (.05 campaign) and sun damage (slip slop slap) campaigns. NAB considers these to be best practice and recommends similar campaigns around cyber security to be developed. Compulsory education at schools and awareness sessions at local community centres should also be undertaken.

NAB also believes that compulsory data breach reporting to Office of the Australian Information Commissioner is also best practice behaviour. This enables consumers to be made aware of data breaches affecting their personal information and helps ensure organisations are accountable for the security of their data.

**25. Would you like to see cyber security features prioritised in products and services?**

Yes. Digital products and services need to be secure by design.

**26. Is there anything else that the Government should consider in developing Australia's 2020 Cyber Security Strategy?**

NAB suggests the Government should:

- Ensure an appropriate amount of funding is available to adequately implement the Strategy;
- Prioritise industries that need urgent attention;
- Acknowledge the fast rate of change and ensure more is done quickly and incrementally rather than relying on traditional strategic planning and governance of government spending;
- Utilise an agile delivery method, encouraging experimentation on smaller initiatives; and
- Remain transparent about initiatives which are not successful.