www.csiro.au

CSIRO Submission 19/692

Australia's 2020 Cyber Security Strategy

Department of Home Affairs

November 2019

Enquiries should be addressed to:

Janet Morgan
CSIRO Digital, National Facilities and Collections
GPO Box 1538 Hobart 7001
[redacted]

Main Submission Author:

Liming Zhu
Research Program Leader
CSIRO Data61

Table of Contents

Table of Contents ..... **ii**
Introduction **3**
Response to Discussion Paper **4**
Question 1 - What is your view of the cyber threat environment? What threats should Government be focusing on? 4
Question 2 - Do you agree with our understanding of who is responsible for managing cyber risks in the economy? 4
Question 3 - Do you think the way these responsibilities are currently allocated is right? What changes should we consider? 5
Question 4 - What role should Government play in addressing the most serious threats to institutions and businesses located in Australia? 5
Question 5 - How can Government maintain trust from the Australian community when using its cyber security capabilities? 6
Question 6 - What customer protections should apply to the security of cyber goods and services? 6
Question 7 - What role can Government and industry play in supporting the cyber security of consumers? 6
Question 8 - How can Government and industry sensibly increase the security, quality and effectiveness of cyber security and digital offerings? 7
Question 9 - Are there functions the Government currently performs that could be safely devolved to the private sector? What would the effect(s) be? 7
Question 10 - Is the regulatory environment for cyber security appropriate? Why or why not? 7
Question 11 - What specific market incentives or regulatory changes should Government consider? 7
Question 12 - What needs to be done so that cyber security is 'built in' to digital goods and services? 7
Question 13 - How could we approach instilling better trust in ICT supply chains? 8
Question 14 - How can Australian governments and private entities build a market of high quality cyber security professionals in Australia? 8
Question 15 - Are there any barriers currently preventing the growth of the cyber insurance market in Australia? If so, how can they be addressed? 8
Question 16 - How can high-volume, low-sophistication malicious activity targeting Australia be reduced? 9
Question 17 - What changes can Government make to create a hostile environment for malicious cyber actors? 9
Question 18 - How can governments and private entities better proactively identify and remediate cyber risks on essential private networks? 9
Question 20 - What funding models should Government explore for any additional protections provided to the community? 9
Question 21 - What are the constraints to information sharing between Government and industry on cyber threats and vulnerabilities? 10
Question 22 - To what extent do you agree that a lack of cyber awareness drives poor consumer choices and/or market offerings? 10
Question 23 - How can an increased consumer focus on cyber security benefit Australian businesses who create cyber secure products? 10
Question 24 - What are examples of best practice behaviour change campaigns or measures? How did they achieve scale and how were they evaluated? 10
Question 25 - Would you like to see cyber security features prioritised in products and services? 11
Question 26 - Is there anything else that Government should consider in developing Australia's 2020 Cyber Security Strategy? 11

Introduction

CSIRO welcomes the opportunity to provide input to the Department of Home Affairs (DHA) on Australia's 2020 Cyber Security Strategy.

Cyberthreats are increasing while our environments are becoming more complex. It is important for Australia to build trust and confidence in our nation's digital economy through mission-driven cybersecurity research, secure research infrastructure and catalysing a cybersecurity industry.

CSIRO has world class research capabilities in cybersecurity and delivers rigorous and comprehensive research in many cybersecurity areas such as trustworthy systems, Internet of Things (IoT) security, human-centred security, Artificial Intelligence (AI) security, information security and privacy. CSIRO also has world-class secure research infrastructure, servicing industry, government and the science community.

In 2016, the Commonwealth Government's **National Innovation and Science Agenda (NISA)** directed CSIRO's Data61 to undertake a range of initiatives aimed at boosting research, commercialisation and connectivity outcomes across Australia's cyber industry and drive the development of new cyber security architectures.

Since then, Data61 has initiated a program of over 47 activities and 6 distinct cyber research themes aimed at driving research and commercialisation and enhancing connectivity and skills development across our organisation and network in Australia. These activities are already having a measurable impact in changing the level of collaboration across our cyber ecosystem and aligning activity around our key cyber challenges and opportunities.

CSIRO's submission to the DHA draws on our broad range of scientific expertise, foresighting/strategic advisory expertise and research infrastructure operation expertise in dealing with cybersecurity across many sectors of activity and with government departments, agencies, research institutions and with the commercial and non-government sectors.

The DHA has asked for responses to their discussion paper on Australia's 2020 Cyber Security Strategy. Our response addresses the twenty-six questions in the discussion paper.

CSIRO welcomes the opportunity to discuss these matters in more depth with the DHA.

Response to Discussion Paper

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

CSIRO suggests that the following threats need to be addressed:

- New cyber threats due to the use of emerging technologies such as:
  - Adversarial examples to fool AI models
  - Training data poisoning
  - Information leakage through model/AI-as-a-service
  - Data integrity attack
  - Database reconstruction attack through publicly released (but poorly "anonymised" or desensitised/redacted) datasets
  - Information warfare/operation using fake or compromised online identity
  - Fake news and deep-fakes (AI-generated images, audios and videos)
- Increased cybersecurity attack points due to increasing data release and sharing
- Stealing sensitive research/Intellectual Property (IP) or sensitive data through semi-open research and collaboration environment.
- Compromising the weakest link (often Small-to-Medium Enterprises (SME) and 3rd party suppliers to main target) on the supply chain.
- Globalisation and the impact on shared services and Data Sovereignty
- Increasing use of Internet of Things (IoT) devices will increase the attack surface.
- Quantum supremacy (i.e. the ability of quantum computers to solve problems that classical computers practically cannot) will have a huge impact of the threat to online services.

In addition, we suggest that there needs to be an improved focus on threats that impact consumers and small businesses as the uptake of consumer and small business oriented connected devices (such as IoT) creates significant risk due to the highly variable levels of cyber security between these user environments.

Furthermore, the cyber security threat landscape needs to be assessed on a sector by sector basis. The cyber security priorities within each sector are different.

As an example, due to life-critical and safety concerns, significant focus should be placed on cyber security for health and medical products. Products that qualify as a medical device are appropriately regulated by the TGA for consumer and professional use, however there are numerous connected & software-based health and wellness products that are unregulated for cyber safety, and as such present a significant threat to Australia.

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

CSIRO suggests that it is unreasonable to expect all end-users to understand the complexities of the cyber threat landscape, or how to respond to a cyber event. Greater consideration needs to be given to ensuring there are mechanisms in place to maintain end-user safety and continued social and economic confidence in the digital world.

In other similarly risky situations, the burden of risk is not on the individual user e.g. informed consent where a person such as a medical practitioner, is given clear safety information from a company as is required under the therapeutic goods Act and is responsible for explaining the risks and benefits to the user. A similar approach could be adopted here.

Through application of the regulatory system it can be made easier for people to safely operate connected devices, and by providing robust services that are usable and have built-in security (security and privacy by design).

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

CSIRO suggests consideration be given to a shift in responsibility for managing a greater portion of cyber risks away from end-users (including SMEs) onto industry and government sectors be contemplated in some scenarios, for example:

1. Encouraging SMEs to innovate on promising secure platforms **for Cyber Assured Software Engineering.**
2. Providing special **managed data/IP security ecosystem** research infrastructure (coupling physical and cyber security) to the wider research ecosystem and SME community for conducting sensitive research and handling sensitive data in both innovation and supply chain.
3. Forming public-private partnerships for providing secure **public data-powered industry platforms** for the wider industry ecosystem. This will responsibly and securely enhance public data with private data and vice versa to create new value from data.
4. Using public-data (e.g. business registries, licensing/certificate information) to provide additional trust to business websites (such as through enhanced DNS services) and business transactions (such as through enhanced smart contracts).
5. Promoting a national approach to protect certain types of highly sensitive but highly valuable data such as **genomics data, cybersecurity data, energy data, telecommunication data, financial systems data**, while extracting value from them in collaborative ways.
6. Increased scrutiny (through legislation and regulation) on the cyber safety of products that are marketed for sale in Australia and ramifications for distributors who market products that do not meet national cyber safety expectations.

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

In addition to the response to question 3, the following could be contemplated:

- Coordinate and collaborate on information sharing in relation to certain types of cyber events such as threat intelligence and response.
- Ensure products that have no baseline safety standards in sectors that have high social and economic value are improved with minimum design and life-of-product safety expectations, with a strong focus on products used by consumers and small business operators. Fundamentally this is a safety issue.
- Develop and implement sector specific strategies that create a cyber secure environment for non-essential but high-value economic activities which increasingly rely on global connectivity and collaboration (e.g. most new technology development).
- Continue to bolster entities such as Computer Emergency Response Team (CERT)'s capability to work with SMEs and individuals to get back on their feet after an incident.

- Provide education and awareness to remove the culture of victim blaming in relation to cyber incidents (as this is one of the reasons that information about cyber-attacks/incidents are not disclosed and shared).

For the education and research sector, more advice could be provided to research organisations around projects that may face greater risk. A significant issue for the sector is insider threat. Advice and assistance on how to manage this threat, as well as support for the verification of overseas researcher identity will be important.

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

CSIRO suggests this can be addressed through transparency about the approaches taken on both the legal and the technical side, developing guiding principles that operate in all circumstances, and by publishing the service's outputs. On the technical side, we suggest partnerships with trusted advisors in the research community be pursued to define the technical approach and risk mitigation strategies. Finally, providing consumers with choices that are supported by appropriate risk-based or compliance-based frameworks.

Question 6 - What customer protections should apply to the security of cyber goods and services?

Generally, consumers don't have the knowledge to make informed decisions regarding the risk: benefit associated with the use of a product or service that may develop a cyber vulnerability. The rate of change in this domain, makes it unreasonable to expect consumers /SMEs to keep up with information on these risks.

CSIRO considers the existing high-level standards and legislation are largely sufficient, however consideration should be given to:

- provision of guidelines and assistance to help with conformance and compliance especially for SMEs (they would also be protected by this), and also in dealing with emerging technologies.
- encouraging a high level of industry professionalism, where individuals/entities performing these services are certified by a centralised accredited body.
- protection of consumers who use devices in line with manufacturers' operating information yet are the target of a cyber event. They should not be responsible for the consequences (e.g. under the Privacy Act) and should have access to some form of protection, for example cyber security insurance.

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

Please see the answers to question 1 for emerging threats and question 3 for government's role. In addition, the following roles are suggested for consideration:

- Compliance/Conformance-by-design reference implementations that are valuable to common use cases and/or using emerging technologies.
- Test cases and automated security compliance checking tools for certain sectors
- IoT security guidelines and IoT product registry.
- Education campaigns on cyber safety, similar to:
  - Workplace health and safety
  - Hand hygiene for health care
- Providing a minimum level of security for industry which Government would enforce (e.g. TGA)

- Appropriate incentives for good security e.g. financial incentives for updating IT systems every X number of years.

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

In addition to the responses to question 3, the TGA could be used as a case study in the following areas:

- Essential principles for safety, quality and performance of a product or service
- Comprehensive guidance for industry
- Post-market expectations (appreciating the risk profile changes over the life cycle of a device)
- Compliance and enforcement

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

Any devolution of functions would need to be carefully assessed to ensure that it would not significantly impact national security, or the economy and there is not a subsequent accessibility issue for people on low incomes.

Question 10 - Is the regulatory environment for cyber security appropriate? Why or why not?

CSIRO recommends that more guidance and clarity as well as sector specific regulation and guidance is required in line with our responses to question 5 and question 7. In addition, we suggest consideration of the promotion of the use of "formal methods" and a **"provably secure"** approach (i.e. using formal mathematical proofs to **prove** software is secure vs. traditional **testing** methods that show systems are **"probably secure"**) for security compliance and build capabilities around it in both industry and government sectors.

Question 11 - What specific market incentives or regulatory changes should Government consider?

CSIRO suggests the following be contemplated:

- Introducing an IoT security rating/guideline systems
- Encouraging SMEs to innovate on promising secure platforms for Cyber Assured Software Engineering
- Encouraging SMEs to use managed data/IP security ecosystem research infrastructure (coupling physical and cyber security) for their innovation and global supply chain integration.
- Introducing financial incentives for small businesses and low-income earners to keep their IT systems cyber secure, e.g. 3-year systems upgrades, training courses, cyber security consultants, etc.
- Introducing regulation and regulatory guidance for essential service providers and authorising appropriate entities to work with essential service providers to develop national safety frameworks.

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

CSIRO suggests the following be contemplated:

- Promote the concept of secure-by-design and the use of “formal methods” and “provably secure” approach (i.e. using formal mathematical proofs to prove software is secure vs. traditional testing methods that show systems are “probably secure”) for security compliance and build capabilities around it in both industry and government.
- Work with sectors to determine reasonable expectations for product and service cyber security and develop sector specific guidance under relevant federal entities to outline how approaches such as secure-by-design, quality-by-design, total-product-life-cycle, and the NIST cyber response framework can dramatically improve the baseline level of security.

Question 13 - How could we approach instilling better trust in ICT supply chains?

See the answers to question 7 which are applicable to SMEs. In addition, CSIRO suggests the following be contemplated:

- Encouraging SMEs to innovate on promising secure platforms for Cyber Assured Software Engineering
- Encouraging SMEs to use managed data/IP security ecosystem research infrastructure (coupling physical and cyber security) for their innovation and global supply chain integration.
- Investing in R&D in supply chain integrity research across key industry sectors, not just ICT industry itself but many ICT-enabled industries such as Agriculture & Food.
- Educating businesses to understand why cyber security needs to be considered as part of their procurement/contracting process.
- Acting on recommendations outlined in AustCyber and CSIRO reports to develop 'trusted ecosystems'.
- Introducing standardised supply chain assessments and documentation by vendors, with a legal requirement to ensure the supply chains are fit for purpose.

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

CSIRO suggests the following be contemplated:

- Focus on investing in human – machine/AI collaboration and efficient ecosystem collaboration as “high quality” aspects.
- Ensure adequate workforce planning activities, including encouragement of professional skills development, micro credentialing and bigger tertiary education cohorts.
- Encourage cyber security as a trade (not everyone needs a Bachelor degree to be a useful cyber security professional - the field changes rapidly).
- Recognise that some sectors (e.g. medicine and engineering) should be including formal education on cyber security (information security and service continuity) as part of their basic bachelor education.

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

CSIRO suggests the following barriers are preventing growth in the cyber insurance market:

- Lack of data and data sharing.
- Lack of risk-mitigation driven adaptive pricing.
- Lack of precedence, limited case studies, confusion from customers on what is being insured and no legislation around what is covered.

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

CSIRO suggests the following be contemplated:

- Recognise the similarities to public health education, use wide spread and straightforward awareness campaigns, not dissimilar to 'slip slop slap', 'wash your hands', etc.
- Leverage the Stay Smart Online - this has worked well when we explain how to stay safe to non-experts.
- Consider sector specific consumer guidance, e.g. as the TGA have for medical device cyber security.
- Consider whole of economy campaigns to ensure that the basics are done right to remove the low hanging fruit issues.

Question 17 - What changes can Government make to create a hostile environment for malicious cyber actors?

CSIRO suggests the following be contemplated:

- Demonstrate enforcement of penalties on cyber offenders and introduce significant legal consequences to deter malicious actors.
- Proactively target and respond to, within defined boundaries, those that target non-commonwealth entities.

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

CSIRO suggests the following be contemplated:

- Ensure efficient, near real time, technology-driven, privacy (including organisation privacy and confidentiality)-preserving sharing of both threat and response information and coordination (vs. forums, meetings and low value threat intelligence sharing).
- Apply the US National Institute of Standards and Technology (NIST) framework and share outcomes and learnings between government and business.
- Develop formal networks for sector specific coordinated vulnerability disclosure.
- Actively work with international bodies that establish best practice for cyber security, for example the TGA's participation in the International Medical Device Regulators Forum (IMDRF).

Question 19 -What private networks should be considered critical systems that need stronger cyber defences?

Our view is that any network associated with an essential/critical service/infrastructure, including key data infrastructure in research organisations, government and industry should be considered for stronger cyber defences.

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

CSIRO suggests the following be contemplated:

- A model similar to the US Small Business Innovation Research (SBIR) program https://www.sbir.gov/about/about-sbir for encouraging innovation on highly secured platform technologies and providing associated training.
- Funding for encouraging SMEs to use managed data/IP security ecosystem research infrastructure (coupling physical and cyber security) for their innovation and global supply chain integration.
- Funding for using public-data (e.g. business registries, licensing/certificate information) to provide additional trust to business websites (such as through enhanced DNS services) and business transactions (such as through enhanced smart contracts).

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

CSIRO suggests the following constraints be addressed:

- concerns around organisational privacy and sensitive information leaks impacting reputation and competitive advantage;
- the lack of efficient mechanisms for coordination and actionable intelligence. Privacy (organisational privacy and confidentiality)-preserving information sharing and government curated datasets for cybersecurity research and innovation are the key areas requiring investment and innovation.
- trust and the lack of ability to appropriately and consistently assess the cyber security posture of organisations.

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

CSIRO agrees to a large extent, but our opinion is that demand drives supply – if more consumers ask for particular features it will drive demand. This could be seen as a market failure which needs government intervention.

Question 23 - How can an increased consumer focus on cyber security benefit Australian businesses who create cyber secure products?

In CSIROs view it will drive more cyber-competitive products for export and increase trust in Australian businesses.

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

CSIRO suggests the following be examples be considered:

- Workplace health and safety
- Hand washing – disease prevention
- Safety in Aviation industry
- Slip Slop Slap – skin cancer awareness
- Put it in the bin – rubbish management

Question 25 - Would you like to see cyber security features prioritised in products and services?

Yes.

Question 26 - Is there anything else that Government should consider in developing Australia's 2020 Cyber Security Strategy?

CSIRO suggests the following be contemplated:

- Leverage the establishments/organisations already in existence. The landscape for managing cyber security at a national level is complex (defence vs civilian, essential services vs others, sector needs, state authorities, etc) and so adding additional government entities will not be helpful.
- Develop a strong understanding of where Australian industry is not cyber secure, or cyber ready. Sectors such as agriculture stand to benefit from the digital economy, however many are still analogue, let alone with any strong cyber security.
- Leverage the efforts of other nations. it would be good to build on other work rather then re-invent it.

CSIRO welcomes the opportunity to discuss these matters in more depth with the DHA (please see contact details on the cover page).