October 2019

Comments on Australia's 2020 Cyber Security Strategy

From the Internet Society

Supporting content

Internet Society

Table of Contents

Introduction 3

1. What is your view of the cyber threat environment? What threats should Government be focusing on? 3

3. Do you think the way these responsibilities are currently allocated is right? What changes should we consider? 5

4. What role should Government play in addressing the most serious threats to institutions and businesses located in Australia? 6

5. How can Government maintain trust from the Australian community when using its cyber security capabilities? 6

Case Study: How can Government proactively address national cyber threats? 9

7. What role can Government and industry play in supporting the cyber security of consumers? 9

8. How can Government and industry sensibly increase the security, quality and effectiveness of cyber security and digital offerings? 10

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

13. How could we approach instilling better trust in ICT supply chains? 11

Introduction

The Internet Society is pleased to submit our comments and suggestions for developing Australia's 2020 Cyber Security Strategy.

The Internet Society is a global not-for-profit organisation that supports and promotes the development of the Internet as a global technical infrastructure, a resource to enrich people's lives, and a force for good in society. Working through a global community of chapters and members, the Internet Society collaborates with a broad range of groups to promote the technologies that keep the Internet secure, and advocates for policies that enable universal access. It is also the organisational home of the Internet Engineering Task Force (IETF) and the Online Trust Alliance (OTA) initiative.

Cyber security is among the topmost concerns for Internet users in the Asia-Pacific region.[1] In response, our priorities continue to include improvements in technical security, through activities such as the Mutually Agreed Norms for Routing Security (MANRS) campaign,[2] and building trust on the Internet, specifically by promoting the security and privacy of the Internet of Things (IoT) ecosystem.[3]

We commend the Australian Government for initiating a multistakeholder process in developing the 2020 Cyber Security Strategy, and highlighting the need for increased cooperation and collaboration among different groups and sectors to address cyber security concerns. We would also like to compliment the Government for taking the lead in cross-border and cross-stakeholder sharing of information about cyber threats, incidents and mitigations. Multistakeholder processes are inclusive and effective, and they reduce the risk of creating a set of priorities that reflect only the interests of any one entity. We have for more than two decades been a strong advocate and facilitator of multistakeholder approaches in policy development and decision-making.[4]

Please find below our responses to the questions posed in the discussion paper. Please note that some of the responses are related to multiple questions, but we have selected the most relevant set of questions to present our responses.

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

The Internet Society recognises Australia's pioneering role in promoting IoT security and privacy, notably the IoT Alliance Australia's (IoTAA) issuance of comprehensive IoT security guidelines in 2017.

[1] Internet users include those in government, private sector, civil society, technical community and academia. Internet Society, Survey on Policy Issues in Asia-Pacific 2019: Consolidation in the Internet Economy, September 2019, https://www.internetsociety.org/resources/doc/2019/the-internet-society-survey-on-policy-issues-in-asia-pacific-2019/.

[2] Internet Society, Improving Technical Security, https://www.internetsociety.org/issues/security/.

[3] Internet Society, Building Trust, https://www.internetsociety.org/issues/trust/.

[4] Internet Society, Multistakeholder, https://www.internetsociety.org/tag/multi-stakeholder/.

We are aware that the IoTAA will be releasing a security testing procedure based on the Internet Society OTA initiative's IoT Trust Framework,[5] which accredited organisations can use as a reference in issuing an IoTAA Security and Privacy Trustmark. We believe these are positive steps towards strengthening the security of IoT systems and protecting consumers' safety, security and privacy.

Nonetheless, IoT-related cyber threats will likely continue to rise at a rapid rate, at least in the short term – a trend that could have devastating effects on Internet users and the Internet's core infrastructure.[6] This is an area that we believe the Australian Government should focus on, working closely with the IoT industry and industry associations, as well as with the technical community, research institutions and consumer protection organisations to identify areas of support.[7]

A survey conducted this year by Consumers International and the Internet Society revealed that over 80% of consumers in Australia want regulators, manufacturers and retailers to take more responsibility and uphold standards of security and privacy, as is the case with other mainstream activities that pose potentially high risks to individuals – such as the safety of air travel.[8]

As a start, the Australian Government, as a large procurer of IoT solutions, could specify a set of security and privacy outcomes for procurement procedures, using the Internet Society OTA initiative's IoT Trust Framework as a guide. When public institutions provide a market for best practices in IoT security, providers have an incentive to respond to meet the demand, thereby benefiting the IoT market at large.

Some countries have introduced policies and guidelines that focus only on the security of IoT devices and systems, but as the Internet Society OTA initiative's IoT Trust Framework outlines, there are benefits to considering IoT security and privacy together. For example, safeguards that limit the amount of data collected and the time it can be kept can reduce the risk of future security breaches.[9] Similarly, encrypting IoT-related data by default – whether at rest or in motion – contributes both to enhancing the security of the IoT system as a whole, and mitigating the privacy risk of harm occurring from data breaches.

[5] Internet Society, OTA IoT Trust Framework, https://www.internetsociety.org/iot/trust-framework/.

[6] According to a study by the Internet Society, it appears unlikely that market-driven security improvements will spread widely and quickly enough to offset the rapid growth, particularly in consumer IoT devices, at least in the short term. Mark McFadden, Sam Wood, Robindhra Mangtani and Grant Forsyth, The Economics of the Security of Consumer-Grade IoT Products and Services, Internet Society, April 2019, https://www.internetsociety.org/resources/doc/2019/the-economics-of-the-security-of-consumer-grade-iot-products-and-services/.

[7] For more information on the risks of insecure IoT devices and systems, see Sections 1 and 2 of: Mark McFadden, Sam Wood, Robindhra Mangtani and Grant Forsyth, The Economics of the Security of Consumer-Grade IoT Products and Services, Internet Society, April 2019, https://www.internetsociety.org/resources/doc/2019/the-economics-of-the-security-of-consumer-grade-iot-products-and-services/.

[8] Consumer International and Internet Society, The Trust Opportunity: Exploring Consumers' Attitudes to the Internet of Things, May 2019, https://www.internetsociety.org/resources/doc/2019/trust-opportunity-exploring-consumer-attitudes-to-iot/.

[9] See: Internet Society, IoT Security for Policymakers, April 2018, https://www.internetsociety.org/resources/2018/iot-security-for-policymakers/; and Internet Society, Policy Brief: IoT Privacy for Policymakers, September 2019, https://www.internetsociety.org/policybriefs/iot-privacy-for-policymakers/.

Since 2018, we have worked with multiple stakeholders in the Canadian Internet community, including the government, to come up with recommendations for policy on IoT security for Canada. The Australian Government may find its outcome report a useful resource.[10] Specifically, we would like to bring to your attention the Shared Responsibility Framework that has been developed from the Canadian process. This framework contains recommendations that need to be communicated to consumers, manufacturers, retailers, service providers, governments, civil society, educational institutions and others, and could be used in IoT-related awareness raising campaigns.[11]

In IoT systems, different components may be under the control of different actors in different jurisdictions (e.g., a server may be located in one country, while the device may be manufactured in another, and in use in yet another), making it difficult to cooperatively solve IoT security issues and making cross-border enforcement challenging. We encourage the Australian Government to join the IoT Security Policy Platform, a collaborative body of government agencies and global organisations working together to harmonise national- and global-level IoT security frameworks, and promote best practices in IoT security to address key challenges to the ecosystem.[12]

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

The Australian Government should play a leading role in: (1) facilitating a collaborative approach to tackling cyber security issues through engagements with the private sector, civil society, academia and other stakeholders, within and across national borders;[13] and (2) increasing capacity building efforts that enhance the resilience and capabilities of individuals and organisations to address cyber security concerns.

We agree that the burden to anticipate and cope with online risks should not fall entirely on users and small businesses, and favour the approach of transferring primary responsibility for managing cyber risks away from end-users and onto industry.

Our study suggests that consumers generally feel that they have some responsibility for securing their own devices, but they also expect tangible actions from manufacturers, retailers and governments. The majority (84%) of Australians in our study agree that manufacturers should only produce connected

[10] Internet Society, Canadian Multistakeholder Process: Enhancing IoT Security –Final Outcomes and Recommendations Report, May 2019, https://www.internetsociety.org/resources/doc/2019/enhancing-iot-security-final-outcomes-and-recommendations-report/.

[11] See pages 9-10 of the Internet Society, Canadian Multistakeholder Process: Enhancing IoT Security – Final Outcomes and Recommendations Report, May 2019, https://www.internetsociety.org/resources/doc/2019/enhancing-iot-security-final-outcomes-and-recommendations-report/.

[12] Internet Society, IoT Security Policy Platform, https://www.internetsociety.org/iot/iot-security-policy-platform/.

[13] See Internet Society, Collaborative Security: An Approach to Tackling Internet Security Issues, April 2015, https://www.internetsociety.org/collaborativesecurity/.

devices that protect security and privacy, and 82% think that retailers should ensure the connected devices they sell have good security and privacy standards.[14]

The development of industry-adopted security guidelines, standards, certifications and trustmarks would contribute to easing the burden on the public sector (see response to question 7). However, this is insufficient. The Australian Government would need to empower consumers and small business users by, for example, ensuring that suppliers provide security and privacy guarantees, and putting in place redress mechanisms and support for consumers and small businesses. In addition, awareness campaigns will be needed, particularly when new standards, certification processes and trustmarks are released.

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

When addressing serious cyber threats, the Internet Society encourages the Australian Government to consider the extraterritorial effects of regulation and legislation. We recommend starting with the cultivation of a broad range of dialogue to understand differing stakeholder perspectives and priorities, and actively consider the role and impact of decisions on these stakeholders, including in other countries. At the same time, it would be important to consider international and regional best practices and norms when shaping Internet-related laws and policies.[15] These could create better outcomes because they have broader participation and are more politically responsive and economically sustainable.

More broadly, any resulting policy on cyber security must be Focused, Informed and Targeted – "FIT" for purpose. Focused implies that the policy is proportionate and mindful of possible unintended consequences. Informed implies that it is based on sound evidence and realistic input about the practicalities of implementation. Targeted means that the policy should achieve its ends with few or no damaging side effects, and in particular without negative impact on the infrastructure of the Internet. Cyber security policies should not hamper innovation, create digital divides and fragment the Internet, nor should they prevent the Internet from evolving as an open technology for everyone.

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

The biggest single step a government can take to maintain trust in its use of cyber security powers is to ensure that those powers are defensive, not offensive: Governments' focus in cyber security should be on a defensive posture that maximises the availability, reliability, resilience and predictability of the

[14] Internet Society, Concerns Over Privacy and Security Contribute to Consumer Distrust in Connected Devices, Press Release, 1 May 2019, https://www.internetsociety.org/news/press-releases/2019/concerns-over-privacy-and-security-contribute-to-consumer-distrust-in-connected-devices/.

[15] Internet Society, The Internet and Extra-Territorial Effects of Laws, September 2018, https://www.internetsociety.org/resources/doc/2018/the-internet-and-extra-territorial-effects-of-laws/.

critical national infrastructure (CNI)--not on seeking to undermine the same qualities in other governments' CNI, or in the Internet infrastructure as a whole.

In this context, a high level of trust in the government's ability to address cyber security risks goes hand in hand with the confidence that under no circumstances will it compromise Internet security as it seeks to achieve these goals. Without this assurance, users are likely to feel vulnerable and reluctant to take advantage of the many benefits that the Internet offers.

A recent global survey of 25 economies (including Australia) found that lack of confidence in security is a leading reason for their distrust of the Internet.[16] Among Australian respondents who said they distrust the Internet, 71% stated that governments contribute to this distrust; with 90% citing cyber criminals, 83% social media companies and 79% foreign governments as the causes of distrust.[17]

To establish a solid foundation of trust to realise the Internet's full potential, it could be helpful to consider four interrelated dimensions when developing policies for the Internet: (1) user trust; (2) technologies for trust; (3) trusted networks; and (4) trustworthy ecosystem.[18]

Encryption is a core building block of a trusted and secure ICT ecosystem. Encryption technologies help keep people safe online by protecting the integrity and confidentiality of digital data and communications.[19] They secure web browsing, online banking, and critical public services like electricity, elections, hospitals and transportation – and every citizen that relies on them.

Unfortunately, there is no digital lock that only law enforcement agencies can open, but those in organised crime cannot. This is technically impossible. Thus, exceptional access measures, such as the power to issue technical capability notices, weaken Australia's security and endanger every citizen. The Australian Government is also putting its economy and the critical services it depends on at greater risk of harm. [20]

The Assistance and Access Act 2018 is a threat to the economy as companies and governments around the globe lose trust in the security of Australian computing products and online services, and the ability to safely host data in the country.[21]

[16] Centre for International Governance Innovation, 2019 CIGI-Ipsos Global Survey on Internet Security and Trust: Detailed Results Tables, p. 22, https://www.ipsos.com/sites/default/files/ct/news/documents/2019-06/cigi-ipsos-2019-dt-6-11-2019_0.pdf.

[17] Centre for International Governance Innovation, 2019 CIGI-Ipsos Global Survey on Internet Security and Trust: Detailed Results Tables, p. 20, https://www.ipsos.com/sites/default/files/ct/news/documents/2019-06/cigi-ipsos-2019-dt-6-11-2019_0.pdf.

[18] Internet Society, A Policy Framework for an Open and Trusted Internet, March 2017, https://www.internetsociety.org/resources/doc/2016/policy-framework-for-an-open-and-trusted-internet/.

[19] Andrew Sullivan, The False Promise of "Lawful Access" to Private Data, WIRED Opinion, 16 May 2019, https://www.wired.com/story/the-false-promise-of-lawful-access-to-private-data/.

[20] Internet Society, Factsheet for Policymakers: 6 Ways "Lawful Access" Puts Everyone's Security At Risk, May 2019, https://www.internetsociety.org/resources/doc/2019/factsheet-for-policymakers-6-ways-lawful-access-puts-everyones-security-at-risk/.

[21] Henry Belot, Microsoft says encryption laws make companies wary of storing data in Australia, ABC News, 28 March 2019, https://www.abc.net.au/news/2019-03-28/microsoft-says-companies-are-no-longer-comfortable-storing-data/10946494; and Paul Smith

Neither will Act prevent terrorists and criminals from using unbreakable encryption developed by foreign companies and independent coders.

The Internet Society urges the Australian Government to protect the use of strong encryption, including end-to-end encryption. It should not require or cause companies to build-in the technical means to provide access to encrypted communications and data.

Allowing any point of entry to a secure service is antithetical to security and to building trust in the digital ecosystem.

For more information regarding these issues, we would like to refer the Australian Government to the following documents from our local chapter, Internet Australia:

- Media Release: Facebook Encryption Letter Contradicts Government's Own Advice for Staying Smart Online Week[22]
- Submission to the Parliamentary Joint Committee on Intelligence and Security on the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018[23]
- Open letter to the Honourable Minister Dutton regarding the Assistance and Access Bill 2018[24]
- Submission to the Department of Home Affairs[25]

We would also like to refer the Australian Government to the following documents from the Internet Architecture Board (IAB):

- IAB comments on the Australian Assistance and Access Bill 2018[26]
- IAB statement on Avoiding Unintended Harm to the Internet[27]

and Bo Seo, Encryption laws a threat to investment: Microsoft, Australian Financial Review, 27 March 2019, https://www.afr.com/technology/encryption-laws-a-threat-to-investment-microsoft-20190327-p51814.

[22] Internet Australia, Facebook Encryption Letter Contradicts Government's Own Advice for Staying Smart Online Week, Media Release, 11 October 2019, https://internet.org.au/news/218-media-release-facebook-encryption-letter-contradicts-government-s-own-advice.

[23] Internet Australia, Submission to the Parliamentary Joint Committee on Intelligence, 11 October 2018, https://www.internet.org.au/images/MediaReleases/2018-10-PJCIS-Assistance-and-Access-Bill-submission---Internet-Australia.pdf.

[24] Internet Australia, Open Letter regarding the Assistance and Access Bill 2018 to the Honourable Minister Dutton, 8 October 2018, https://www.internet.org.au/images/MediaReleases/2018-10-Open-Letter-Hon-Peter-Dutton-MP---Internet-Australia.pdf.

[25] Internet Australia, Submission to the Department of Home Affairs, 10 September 2018, https://www.internet.org.au/images/MediaReleases/2018-09-DOHA-Assistance-and-Access-Bill-Submission---Internet-Australia.pdf.

[26] IAB, Comments on the Australian Assistance and Access Bill 2018, 9 September 2018, https://www.iab.org/wp-content/IAB-uploads/2018/09/IAB-Comments-on-Australian-Assistance-and-Access-Bill-2018.pdf.

[27] IAB, Avoiding Unintended Harm to Internet Infrastructure, 4 September 2019, https://www.iab.org/documents/correspondence-reports-documents/2019-2/avoiding-unintended-harm-to-internet-infrastructure/.

Case Study: How can Government proactively address national cyber threats?

In the case study, the Australian Government considers proactively identifying vulnerable systems to assess Australia's exposure to threats. The Internet Society would like to urge the Australian Government to exercise care and make sure that the assessment does not create security and privacy risks.

Resorting to measures like active probing of user-owned machines to test their security by attempting to log in using well-known default passwords, for example, raises significant security and privacy concerns:[28]

- Active probing without the knowledge and permission of the device owner, irrespective of the motivation, is a technical attack on that device;
- The device owner has no way to distinguish a malicious attack from an “authorised” legitimate one, and might therefore react inappropriately to a legitimate probe, or fail to react appropriately to a malicious one. This may give rise to unintended and undesirable outcomes. For instance, if users are warned via a general announcement that “legitimate probes will be conducted overnight on Thursday of next week,” hackers might interpret that as an opportunity to launch their own attacks, in the knowledge that device owners are less likely to react;
- It could result in the creation of a large database of vulnerable devices, which would be both a target and an asset for potential attackers. Creation of such an asset should not be done without caution and forethought;
- Probing could cause the devices to fail, carrying additional risks for the owner and/or user of the device; and
- It is even possible that an active probe could infringe the sovereignty of another nation or the rights of its citizens.

Overall, our view is that the active probe approach carries a high risk of undermining users’ trust in the Internet, particularly by breaching the normal expectations of the device owners and users concerning privacy, ownership and control. Actively testing device security by attempting to log in using well-known default passwords should be a last resort, in light of a specific, identified threat, and used only when other alternatives[29] are not available or practical.

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

[28] Steve Olshansky and Robin Wilton, Internet of Things Devices as a DDoS Vector, Internet Society, 11 April 2019, https://www.internetsociety.org/blog/2019/04/internet-of-things-devices-as-a-ddos-vector/.

[29] As a simple example, one alternative would be laboratory testing of devices to check whether they insist on a password change when installed, and whether they test for strong passwords, followed by a warning to the manufacturer if this is not the case.

Industry bodies and policymakers should prioritise raising cyber security awareness, and incorporate cyber security literacy in all digital literacy programmes.

Awareness campaigns could motivate consumers to assess the security of products they consider purchasing. Yet in the IoT sphere, research has shown that such intervention will not be sufficient to have a real impact on consumer decisions, especially when buying an IoT product.[30] A key reason is that manufacturers do not systematically communicate information about the security features that devices possess. The average consumer does not have the expertise required to evaluate this information, and typically is inclined to avoid such demanding tasks. A well-known and understood label or trustmark that consumers can relate to is a more achievable intervention that could influence their choices.

The Internet Society is supportive of Australia's efforts towards testing and certifying IoT products and services, and developing an industry-supported trustmark. According to a global survey on Internet security and trust, 93% of Australians indicated that they would be more confident buying a product that has a security certification mark.[31]

A trustmark could facilitate consumers' ability to distinguish between devices at point of purchase, and neatly embodies detailed information. This would help empower consumers (which can be either individuals, businesses or governments) to demand products and services that have been designed with cyber security in mind. It is a complement to raising cyber security awareness. At the same time, a trustmark could incentivise manufacturers to compete on security as a form of market differentiation. It would also establish an industry process to agree on security standards, and hold manufacturers to account by directing their attention to the security of devices according to clear criteria and guidelines. Finally, a trustmark would facilitate market and consumer protection oversight of compliance to IoT security in a more consistent and transparent way.

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

One suggested measure for IoT is to mandate adherence to a minimum set of industry-developed security and privacy standards that connected devices and services must meet before they can be manufactured, imported or sold in the country.

But rather than a rigidly-specified set of prescribed standards that would not be easily adapted as IoT evolves, this could involve compliance with principles or outcomes, such as: (1) no universal or easily guessed pre-set passwords; (2) data should be transmitted and stored securely using strong encryption; (3) data collection should be minimised to only what is necessary for a device to function; (4) devices

[30] Internet Society, Canadian Multistakeholder Process: Enhancing IoT Security – Final Outcomes and Recommendations Report, May 2019, https://www.internetsociety.org/resources/doc/2019/enhancing-iot-security-final-outcomes-and-recommendations-report/.

[31] Centre for International Governance Innovation, 2019 CIGI-Ipsos Global Survey on Internet Security and Trust: Detailed Results Tables, p. 96, https://www.ipsos.com/sites/default/files/ct/news/documents/2019-06/cigi-ipsos-2019-dt-6-11-2019_0.pdf

should be capable of receiving security updates and patches; (5) device manufacturers should notify consumers if there is a security breach; and (6) device manufacturers should ensure consumers are able to reset a device to factory settings in the event of a sale or transfer of the device.

This principles-based approach should lead to improved security while retaining flexibility for the market to innovate and improve on security measures. It also helps to future proof policies so that they will not need to be significantly changed with new technologies.

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

Regulatory changes to consider include reducing the legal risks faced by security researchers looking to responsibly disclose information on software vulnerabilities they have discovered, and proactively prosecuting manufacturers or service providers who make misleading claims on security. Further, Australian cryptography and security researchers should be able to communicate their knowledge, expertise and findings with their counterparts in other countries. Any policy or legal obstacles to the smooth collaboration of academic research across borders should be avoided.

The Australian Government could also consider reviewing liability for IoT privacy and security incidents, and, where possible, clearly assigning liability on those that are most able to exercise control over the security and privacy of online products and services, in cases where minimum security practices are not implemented. Clear liability could be an incentive for stronger security. Where existing legal liability mechanisms are unclear, this may lead to uncertainty among consumers and companies involved as to who is responsible and what remedies (including compensation) are available when something goes wrong.

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

The Internet Society would like to compliment the Australian Government for embracing "security-by-design" as a foundational principle to guide enterprises in formulating policies and implementing measures to bolster and reinforce trust in the Internet ecosystem.

We would like to suggest that the Australian Government do not view privacy issues as separate from cyber security, and ensure that enterprises also incorporate "privacy by design" principles. The term "trust by design" includes both security by design and privacy by design principles to ensure that both security and privacy measures are embedded into the architecture of ICT systems and business practices.[32]

[32] Steve Olshansky, The Internet of Things: Why 'Trust By Design' Matters, Internet Society, 24 April 2019, https://www.internetsociety.org/blog/2019/04/the-internet-of-things-why-trust-by-design-matters/. See also the United States National Telecommunications and Information Administration's (NTIA) ongoing work on software component transparency https://www.ntia.doc.gov/SoftwareTransparency

Please send comments and feedback to:

Internet Society - Asia-Pacific Bureau
9 Temasek Boulevard
#09-01 Suntec Tower 2
Singapore 039898

[redacted]

Website – https://www.internetsociety.org/apac
Facebook – /isocasiapacific/
Twitter – @ISOCapac
LinkedIn – https://www.linkedin.com/company/internet-society-apac/
Subscribe to newsletter – http://bit.ly/ISOC-APAC-signup