Australia's 2020 Cyber Security Strategy – A call for views

Submission by the Australian Communications Consumer Action Network to the Department of Home Affairs

31 October 2019

Australian Communications Consumer Action Network (ACCAN)
Australia's peak telecommunications consumer organisation
PO Box 639, Broadway NSW 2007
Tel: (02) 9288 4000 | Fax: (02) 9288 4019 | Contact us through the National Relay Service
www.accan.org.au | info@accan.org.au | twitter: @ACCAN_AU

About ACCAN

The Australian Communications Consumer Action Network (ACCAN) is the peak body that represents all consumers on communications issues including telecommunications, broadband and emerging new services. ACCAN provides a strong unified voice to industry and government as consumers work towards communications services that are trusted, inclusive and available for all.

Consumers need ACCAN to promote better consumer protection outcomes ensuring speedy responses to complaints and issues. ACCAN aims to empower consumers so that they are well informed and can make good choices about products and services. As a peak body, ACCAN will represent the views of its broad and diverse membership base to policy makers, government and industry to get better outcomes for all communications consumers.

Contact

Meredith Lea
Disability Policy Adviser

PO Box 639,
Broadway NSW, 2007
Email: info@accan.org.au
Phone: (02) 9288 4000
Fax: (02) 9288 4019
Contact us through the National Relay Service

Contents

1. Introduction

ACCAN thanks the Department of Home Affairs (the Department) for the opportunity to contribute to Australia's 2020 Cyber Security Strategy. ACCAN appreciates that the Department is working to a tight timeframe for this consultation, and offers our ongoing engagement to ensure that the voices and experiences of consumers are appropriately reflected in Australia's new Cyber Security Strategy.

In our following response to the discussion paper, ACCAN does not offer technical solutions to cyber security concerns, nor are we able to offer detailed answers to each question in turn. Instead, we consider the concerns of consumers, including small businesses, in relation to cyber security, and offer solutions that may help to improve the safety of cyberspace. In addition to the points we raise below, the actions in the existing Cyber Security Strategy that are ongoing or have been revised must be addressed in the new Cyber Security Strategy. Clear explanations must be given as to why these actions were not completed (or were altered), what barriers were encountered and what efforts will be made to ensure that all new actions under the 2020 Cyber Security Strategy will be appropriately prioritised, resourced, and completed.

1.1. List of recommendations

Recommendation 1: Consumer protection must be a key focus of the 2020 Cyber Security Strategy.

Recommendation 2: The 2020 Cyber Security Strategy must clearly outline the responsibilities of governments and industry in relation to identifying and minimising the risk of cyber threats to consumers.

Recommendation 3: The 2020 Cyber Security Strategy must include financial incentives for manufacturers and software developers to increase the security features of connected devices and services.

Recommendation 4: The 2020 Cyber Security Strategy must incorporate specific actions addressing consumer concerns about their privacy and data security.

Recommendation 5: The 2020 Cyber Security Strategy must be future-focussed and adaptable to emerging technologies and associated cyber threats.

Recommendation 6: The 2020 Cyber Security Strategy must fund an accessible and inclusive cyber safety consumer education campaign, to be provided in a range of formats, to inform the general public about cyber security and how to safely navigate the online environment.

Recommendation 7: The 2020 Cyber Security Strategy must call for an appraisal of core school curriculums to consider the extent to which cyber security education is embedded into all levels of schooling.

Recommendation 8: The 2020 Cyber Security Strategy must assign responsibility to industry for providing information to consumers about the security features of connected devices.

Recommendation 9: The 2020 Cyber Security Strategy must call for the development of industry-wide 'security by design' standards to a) improve the base-level security of all connected devices and b) improve consumers' access to information about the security of goods and services.

Recommendation 10: The 2020 Cyber Security Strategy must consult with consumers, Internet of Things experts and industry to consider the feasibility of a 'trust' label for connected devices to support consumers to make more informed purchases.

Recommendation 11: The 2020 Cyber Security Strategy must stipulate the development of a whole of government procurement policy detailing minimum cyber security features for connected devices.

Recommendation 12: The roles and responsibilities of government, industry, regulators and consumers must all be clearly demarcated in the 2020 Cyber Security Strategy with regard to collaborative approaches seeking to prevent cyberattacks and cybercrime.

Recommendation 13: The 2020 Cyber Security Strategy must recognise, reflect and build upon international cyber security efforts.

Recommendation 14: The 2020 Cyber Security Strategy must strengthen international cooperation regarding cyber security incidents, and must improve Australia's capacity to respond to such international cyber security incidents.

1. Responses

1.1. Telecommunication consumer concerns

Considerable efforts must be made to protect the essential services offered by the telecommunications industry. The critical infrastructure of telecommunications must be protected, as must the valuable consumer data that telecommunications companies are responsible for communicating and storing. As is the case in other sectors, telecommunications providers face substantial cyber threats, including Distributed Denial of Service (DDoS) attacks and attacks on infrastructure equipment, such as routers from Internet Service Providers (ISPs). Given the number of connected devices and systems that consumers use and often rely upon, sometimes in relation to the provision of health care or support for people with life-threatening illnesses, there are very real consequences for cyberattacks emerging from a lack of cyber security. Similarly, cyber security incidents can result in considerable costs to small businesses, and by extension, the economy more generally. The impact that cyber security can have on telecommunications consumers, including small businesses, must therefore be acknowledged in Australia's 2020 Cyber Security Strategy.

1.1.1. Risks to consumers

With advances to technology, improvements to digital inclusion within Australian society,[1] and ever more government services moving online, it is vital that consumers are appropriately protected and supported in their online activities. As outlined in the discussion paper, consumers, including small businesses, often bear the cost of cybercrime and malicious online activity. Some reports estimate that the impact of cybercrime on individuals and businesses in Australia costs around $7 billion each year.[2] ACCAN is concerned about the disproportionate impact that scams and other cybercrimes have on vulnerable consumers, such as those who are not confident users of the internet, older people, and people who have less familiarity with the English language.[3]

In addition, small businesses may be ill-equipped to respond to cyber threats, particularly those attacking the availability of their data or attacking their integrity. They may not have the technical skills required to back up important data and information, and may not be aware of how to keep their computers, websites and other systems up to date with software updates or patches. It can be quite costly for small businesses to get their affected systems back up and running after an attack, in addition to the possible business losses they may have incurred as a result of the cyber security incident.

Currently there is too much onus on consumers to manage cyber risks and bear the costs associated with cyberattacks or data breaches. While some consumers believe that they themselves are responsible for their own data privacy, others believe that industry or

[1] As outlined in the 2019 latest Australian Digital Inclusion Index report, available: https://digitalinclusionindex.org.au/

[2] Manuel, D. 2019 'Seven ways the government can make Australians safer – without compromising online privacy', The Conversation, February 28 2019, available: https://theconversation.com/seven-ways-the-government-can-make-australians-safer-without-compromising-online-privacy-111091

[3] ACCAN, 2019 'Response to Discussion paper: Combating scams – technological solutions', ACCAN, available: https://accan.org.au/our-work/submissions/1604-acma-scam-technology-consultation

governments are better equipped to deal with data privacy issues,[4] and expect government to regulate how companies use data.[5] ACCAN strongly believes that networks and industry are better placed than consumers to identify and minimise the risk of scam activity or other cyber threats.[6] The 2020 Cyber Security Strategy must therefore include actions designed to support and protect individuals and businesses, especially smaller businesses that may not have the capacity to invest substantial resources into protecting their business or consumers online.

Recommendation 1: Consumer protection must be a key focus of the 2020 Cyber Security Strategy.

Recommendation 2: The 2020 Cyber Security Strategy must clearly outline the responsibilities of governments and industry in relation to identifying and minimising the risk of cyber threats to consumers.

1.1.2. Information Asymmetry

While more and more Australians are moving online, this is not happening at the same rate for all cohorts of society. There remains a digital inclusion gap for certain groups, such as people with lower levels of income, education and employment, people with disability and people over the age of 65.[7] It is therefore unreasonable to expect that all consumers will actively engage with issues relating to cyber security. It is similarly unreasonable to presume that consumers and small businesses have the skills required to appropriately protect themselves from cyber threats.

> *'In many cases, end users are not fully aware of the dangers of interacting online, and to exacerbate the issue, security experts provide them with too complicated information, often evoking emotions of fear and despair.'*[8]

Information asymmetry between consumers and the manufacturers of digital goods can mean that consumers are not able to make purchase decisions based on the security features of different devices. Many consumers do not have the technical skills or knowledge required to assess the cyber security of different devices,[9] and consumers may expect that the internet connected devices being sold to them are cyber safe. Similarly, consumers engaging with different providers do not always know the quality of the providers' cyber

---

[4] Von Gravrock, E. 2019 'Who should be responsible for protecting our personal data?', World Economic Forum, available: https://www.weforum.org/agenda/2019/01/who-should-take-charge-of-our-cybersecurity/

[5] Ingram, S. 2017 'Protect.me: How consumers see cyber security and privacy risks', PwC, available: https://www.digitalpulse.pwc.com.au/report-protect-me-consumers-cyber-security/

[6] ACCAN 2019 op cit. p2

[7] Thomas, J., Barraket, J., Wilson, C.K., Rennie, E., Ewing, S., and MacDonald, T. 2019 'Measuring Australia's Digital Divide: The Australian Digital Inclusion Index 2019', RMIT University and Swinburne University of Technology, Melbourne, for Telstra, available: https://apo.org.au/sites/default/files/resource-files/2019/09/apo-nid255341-1386471.pdf

[8] Bada, M., Sasse, A. M., and Nurse, J. R. C. 2014 'Cyber Security Awareness Campaigns: Why do they fail to change behaviour?' International Conference on Cyber Security for Sustainable Society 2015, p5. Available: https://arxiv.org/ftp/arxiv/papers/1901/1901.02672.pdf

[9] Houses of Parliament Parliamentary Office of Science and Technology, 2019 'Cyber Security of Consumer Devices', POSTnote number 593 February 2019 p3, available: https://apo.org.au/sites/default/files/resource-files/2019/02/apo-nid219166-1331041.pdf

security practices and protections.[10] A great deal of trust is therefore placed in providers and manufacturers of digital goods and services,[11] yet consumer expectations regarding cyber security are not always met, and trust can be broken.

Consumer surveys and focus groups have indicated that consumers can underestimate the cyber risks they face when using connected devices.[12] This is concerning given that manufacturers often under-invest in security measures.[13] This information asymmetry can in turn impact the market for cyber secure products and services. The findings of an Australian survey illustrated this, outlining that:

> *'Three-quarters of consumers said they expected additional security and privacy to be designed into their connected devices… [Despite this,] only 32 percent were willing to pay a higher price for more secure devices. This creates a challenge for device manufacturers, with consumers expecting a high level of data security, but not necessarily being prepared to pay for it'*[14]

While this may be the case for some consumers, others may wish to purchase more secure devices but may not have the financial means to do so. It is crucial to consider the cost of secure connected devices within this context, as affordability barriers may force some consumers into purchasing less secure (and cheaper) devices when they would prefer to buy more secure (and more costly) devices. Indeed, for some consumers cheaper yet less secure devices may be the only affordable way that they can remain connected. This may in turn place consumers who cannot afford more secure devices at disproportionate risk of experiencing cyber security incidents.

1.1.3. Lack of manufacturer incentives

In acknowledging that some consumers are unable to afford connected devices with strong cyber security features, there remain some consumers who may be able to afford these features but may not prioritise them when making purchases. If consumers are unable to distinguish which devices and services have strong cyber security features[15] and information about these features is not readily provided to them, it is not surprising that consumers may be unwilling to pay extra for cyber security features. Manufacturers consequently have limited incentives to invest more heavily in additional security features for their goods and services.[16] Indeed, in a 2018 report the UK Government 'concluded that manufacturers lack

---

[10] Serabian, D. 2015 'Consumer Protection and Cybersecurity: The Consumer Education Gap', p4 available: https://digitalscholarship.unlv.edu/cgi/viewcontent.cgi?article=1032&context=brookings_pubs

[11] Burt, A. 2019 'Cybersecurity Is Putting Customer Trust at the Center of Competition.' Harvard Business Review. Available: https://hbr.org/2019/03/cybersecurity-is-putting-customer-trust-at-the-center-of-competition

[12] Houses of Parliament Parliamentary Office of Science and Technology, 2019 op cit. p3.

[13] McFadden, M., Wood, S., Mangtani, R., and Forsyth, G. 2019 'The economics of the security of consumer-grade IoT products and services', available: https://www.internetsociety.org/wp-content/uploads/2019/04/The_Economics_of_Consumer_IoT_Security.pdf; see also Sivaraman, V., Habibi Gharakheili, H. & Fernandes, C. 2017, Inside job: Security and privacy threats for smart-home IoT devices, Australian Communications Consumer Action Network, Sydney.

[14] KPMG Australia, 2019 'Consumer Loss Barometer: The economics of trust', p14, available: https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/03/consumer-loss-barometer-2019.pdf

[15] McFadden et.al 2019 op cit.

[16] Ibid.

sufficient economic incentive to incorporate security features into devices.'[17] Instead of spending additional money and time to increase the security of a product or service, manufacturers often prioritise getting their products to market quickly, and for a lower price.[18] This rush to the market is supported by the increased demand for connected devices.[19] Furthermore, manufacturers do not typically wear the costs if a consumer's device or service experiences a security breach or cyber-attack, meaning that they have few (if any) financial incentives to increase the in-built security features of their goods or services.

Recommendation 3: The 2020 Cyber Security Strategy must include financial incentives for manufacturers and software developers to increase the security features of connected devices and services.

1.1.4. Threats to consumer privacy

With research showing that security is often lacking in consumers' connected devices, such as smart TVs, connected door locks, home alarms and thermostats, consumers are becoming increasingly aware of the privacy threats associated with these goods and services.[20] Privacy is an essential human right, and holds significant social and economic value to consumers.[21] Where privacy is not upheld, consumers face substantial detriment – they may lose personal security; they may face economic loss (either directly or indirectly); and may feel exploited by the entity responsible for the breach of their privacy.[22] Indeed, research has found that more consumers would consider changing providers if their mobile provider misused consumer data, compared to the number of consumers who would consider changing providers if their mobile provider was hacked.[23] Consumers report that they are uncomfortable not only with the misuse of their data, but also the way in which businesses or organisations address their concerns about privacy and data security.[24]

Recent research has also shown that smartphone users are concerned about the privacy implications of apps collecting and tracking their location metadata (or geodata).[25] Indeed, survey respondents were more likely to report negative feelings and attitudes (as opposed to positive attitudes) towards apps collecting their location data.[26] Some respondents also stated that they considered the trustworthiness of an app and what benefits they would gain through allowing location services when determining whether or not they would use a certain app or allow it to access their location data. Overall, smartphone users generally felt that

[17] Houses of Parliament Parliamentary Office of Science and Technology 2019 op cit. p3.
[18] McFadden et.al 2019 op cit.
[19] Sivaraman, V., Habibi Gharakheili, H. & Fernandes, C. 2017, Inside job: Security and privacy threats for smart-home IoT devices, Australian Communications Consumer Action Network, Sydney. p13
[20] Ibid; see also: Von Gravrock, E. 2019 op cit.
[21] ACCAN, 2018 'Treasury Laws Amendment (Consumer Data Right) Bill 2018 Consultation – Submission by the Australian Communications Consumer Action Network', ACCAN, available: https://accan.org.au/our-work/submissions/1536-consumer-data-right-submission
[22] Ibid.
[23] KPMG Australia, 2019 op cit. p18.
[24] Ibid, p5.
[25] Riedlinger, M., Chapman, C., and Mitchell, P.2019 'Location awareness and geodata sharing practices of Australian smartphone users', Digital Media Research Centre, Queensland University of Technology. Available from https://eprints.qut.edu.au/132000/
[26] Ibid p25.

service providers and regulators should do more to protect users against privacy risks, with some also suggesting compensation for privacy violations.[27]

Recommendation 4: The 2020 Cyber Security Strategy must incorporate specific actions addressing consumer concerns about their privacy and data security.

1.1.5. Emerging cyber security risks

Given the rate of technological change, the 2020 Cyber Security Strategy must be future-focussed and consider the known and unknown emerging technologies that may impact on Australia's cyber security. For instance, the Cyber Security Strategy must address consumer concerns in relation to the security challenges that 5G technologies will bring. As with all new technologies, there are fears and misunderstandings around 5G, and the Cyber Security Strategy must ensure that its actions appropriately address these fears, clearly outline the risks involved with 5G and offer concrete suggestions for how these risks can be mitigated. Given that 5G will encourage the expansion of interconnected devices and services, while also possibly increasing the potential, speed and intensity of cyber threats, strategies must be put into place to address any arising threats and risks as a matter of priority.

Recommendation 5: The 2020 Cyber Security Strategy must be future-focussed and adaptable to emerging technologies and associated cyber threats.

1.2. Solutions to address Consumer Concerns

Overall, the 2020 Cyber Security Strategy must use multifaceted approaches to address each of the abovementioned consumer concerns. The approaches must from their outset acknowledge and respond to the fact that not all online users have the same level of knowledge or digital skills, and that additional supports may be required by some cohorts. The Cyber Security Strategy must have consumer protections embedded throughout, must recognise the concerns that consumers have around the security of technology,[28] and must acknowledge that cyber security is a shared responsibility. ACCAN believes that the 2020 Cyber Security Strategy should prioritise the creation and maintenance of aware, informed and well-protected consumers. We acknowledge that significant collaboration, between government, industry, consumers and international entities, is required to achieve this goal.

1.2.1. Awareness raising and education

Firstly, accessible and inclusive cyber safety education is required to support all members of the community to safely navigate the online environment. Such education must be practical and relevant, and should inform consumers about how to recognise a cyber threat, what to do if one eventuates, where to go for help if required, and how to report their experiences. Consumer education material should be tailored to different groups in recognition of the differing levels of digital inclusion or confidence that different cohorts may have, and must be made available in a range of accessible formats. Some consumers, for instance, may be confident users of the internet, and may consider themselves to be fairly competent in dealing with IT issues, and yet may remain unaware of how to deal with a cyber threat or may be taken by surprise by a cyberattack.

---

[27] Ibid pp10, 42.
[28] KPMG Australia, 2019 op cit. p16.

Indeed, ACCAN is aware of a recent cyberattack experienced by a small organisation with reasonable technical and digital skill. This small business reported experiencing a ransomware attack on their infrastructure which rendered a server and certain computers non-responsive. Fortunately this small organisation had sufficient technical skills on staff to remove the affected machines and server from the network, quarantine the network, and perform extensive testing which prevented further damage. Regardless, the down time and subsequent days of testing, diagnosis and analysis of the issue was time and labour intensive, and a considerable cost to the business.

All information regarding cyber security must be provided in plain English, both on- and off-line, and through a mixed-media approach – including internet, newspaper, television and radio advertisements, hard-copy brochures and distributing information to community hubs, groups and support services. To ensure that the most vulnerable cohorts also benefit from this education, information must also be provided via non-English speaking television or radio programs, or non-English speaking community groups. A consumer education campaign could also be accompanied by greater inclusion of cyber security within the curriculum across all levels of schooling.[29]

Recommendation 6: The 2020 Cyber Security Strategy must fund an accessible and inclusive cyber safety consumer education campaign, to be provided in a range of formats, to inform the general public about cyber security and how to safely navigate the online environment.

Recommendation 7: The 2020 Cyber Security Strategy must call for an appraisal of core school curriculums to consider the extent to which cyber security education is embedded into all levels of schooling.

While government has a role to play in providing this education to help consumers understand and respond to cyber risks, industry must also take responsibility for raising consumer awareness of the security issues associated with connected devices and services.[30]

> *'Providing information to consumers on the possible impacts of insecure devices and the need for them to seek out secure devices and services will empower consumers to make better buying decisions and help correct information asymmetry in the market.'*[31]

Such consumer awareness must also address gaps in knowledge around security updates, and what the implications are for the consumer when a connected device can no longer be patched with regular security updates.[32] Correcting the current information asymmetry about cyber security and the security features of connected goods and services will help consumers to make cyber-smart choices and demand better security features when making purchases. The asymmetry of information must also be addressed through enforceable consumer protections and incentivising manufacturers to incorporate security features from the start.

---

[29] Manuel, 2019 op cit.
[30] McFadden et.al, 2019 op cit.
[31] Ibid.
[32] Sivaraman, V., Habibi Gharakheili, H. & Fernandes, C. 2017, Inside job: Security and privacy threats for smart-home IoT devices, Australian Communications Consumer Action Network, Sydney. p23

Recommendation 8: The 2020 Cyber Security Strategy must assign responsibility to industry for providing information to consumers about the security features of connected devices.

1.2.2. Cyber security standards

Cyber security principles or standards that embed a 'security-by-design' or 'in-built security' philosophy must be developed to ensure that manufacturers of connected products consider security 'at all stages of product development, sale and ongoing support.'[33] This would go some way towards meeting the Commonwealth Cyber Declaration's requirement that member states work towards user security by default.[34] Security by design standards could improve consumer security by establishing a minimum set of security requirements for connected devices and services and would additionally reduce 'the burden on consumers to ensure that their devices are secure.'[35]

Recommendation 9: The 2020 Cyber Security Strategy must call for the development of industry-wide 'security by design' standards to a) improve the base-level security of all connected devices and b) improve consumers' access to information about the security of goods and services.

Some authors have suggested that the introduction of a standard could in turn lead to the development of a 'trust' label indicating that a device meets minimum security standards.[36] While this could support consumers to differentiate between connected devices based on security features and may offer manufacturers clearer incentives for better security features, it may be difficult to maintain. Indeed, enforcing a 'trust' label is made even more difficult given that security threats are continuously evolving and emerging.[37] Nevertheless, a 'trust' label should be carefully considered and discussed with consumers to ensure any certification scheme introduced to Australia will be of benefit to people purchasing and using connected devices.

Recommendation 10: The 2020 Cyber Security Strategy must consult with consumers, Internet of Things experts and industry to consider the feasibility of a 'trust' label for connected devices to support consumers to make more informed purchases.

1.2.3. Procurement

The government must use its substantial buying power and influence by clearly detailing minimum security features for internet connected devices within its public procurement policies and procedures. This can further incentivise manufacturers to increase the cyber security features inbuilt into their products and services.

> *'These improvements in security may spill over into the consumer market – it may be easier or cheaper for manufacturers to include the same*

[33] Ibid.
[34] Commonwealth Cyber Declaration – United Kingdom, 2018.
[35] Houses of Parliament Parliamentary Office of Science and Technology, 2019 op cit., p3.
[36] Ibid, p4. See also: McFadden et al., 2019 op cit.
[37] Sivaraman et.al op cit. p22.

> *(improved) security measures in all their products, including consumer products.'*[38]

Government procurement standards for cyber security features would help to build cyber security into digital goods and services within Australia, strengthening security for individual consumers and businesses. This could in turn help certain partnerships between small, medium and large businesses and could improve resiliency to cyber incidents by maintaining consistent security standards throughout supply chains.

Recommendation 11: The 2020 Cyber Security Strategy must stipulate the development of a whole of government procurement policy detailing minimum cyber security features for connected devices.

1.2.4. Collaborative approaches to cyber security

National and international collaboration is vital and will assist in the management of cyber security risks. Indeed, treating cyber security as a public good[39] necessitates collaboration, shared responsibility, and joint investments of time and resources. Collaborative approaches allow for cyber security skill and knowledge sharing between and amongst different groups (including individual consumers, small, medium and large businesses, manufacturers, government, regulators, law enforcement etc.) to facilitate more appropriate responses to consumer experiences. This helps different entities within the cyber security system, including individual consumers, to better understand their roles and responsibilities in relation to protecting against cyber threats.[40]

Recommendation 12: The roles and responsibilities of government, industry, regulators and consumers must all be clearly demarcated in the 2020 Cyber Security Strategy with regard to collaborative approaches seeking to prevent cyberattacks and cybercrime.

The Commonwealth Cyber Declaration requires that member states work towards 'common standards, harmonised legal approaches and improved interoperability.'[41] Consideration must therefore be given to the work that is occurring internationally, such as in the UK,[42] in relation to 'secure by design' principles, minimum security standards and procurement policies. The Commonwealth Cyber Declaration similarly requires member states to:

> *'Commit to exploring options to deepen cooperation on cybersecurity incidents and responses between Commonwealth member countries, including through the sharing of information about threats, breaches, vulnerabilities, and mitigation measures'*[43]

Recommendation 13: The 2020 Cyber Security Strategy must recognise, reflect and build upon international cyber security efforts.

---

[38] McFadden et al., 2019 op cit.
[39] Taddeo, M., and Bosco, F. 2019 'We must treat cybersecurity as a public good. Here's why.' World Economic Forum, available: https://www.weforum.org/agenda/2019/08/we-must-treat-cybersecurity-like-public-good/
[40] Ibid.
[41] Commonwealth Cyber Declaration – United Kingdom, 2018 op cit.
[42] Houses of Parliament Parliamentary Office of Science and Technology, 2019 op cit., p1.
[43] Commonwealth Cyber Declaration – United Kingdom, 2018 op cit.

Recommendation 14: The 2020 Cyber Security Strategy must strengthen international cooperation regarding cyber security incidents, and must improve Australia's capacity to respond to such international cyber security incidents.

1.2.5. Improving consumer trust

Finally, consideration must be given to how consumer data is handled and stored by industry, particularly in relation to consumer trust and expectations in relation to data protection and privacy. A recent survey, for instance, found that 88% of consumers would base their willingness to share personal data with a company on how much they trusted it.[44] Research has also shown that 57% of consumers are more likely to use or recommend companies that let them decide how their personal data is used.[45] An Australian survey of smartphone users similarly found that many respondents valued transparency and wanted service providers to take more responsibility.[46] As such, there are industry and consumer benefits for providing consumers with clear and transparent information about how their data is being used, how it is being protected, and what systems are in place to keep them informed about the security of their data.[47] Having procedures or policies in place to govern this information provision, and making this available to consumers, could assist in consumer decision-making and expectation-setting in relation to data breach responses.[48]

Australia has a mandatory data breach notification regime which helps to keep consumers informed about data breaches. Consumers should be consulted in relation to the breadth of information they would like to know in the event of a data breach. This is particularly important given survey findings that security executives and consumers have differing views on what information consumers would like to receive.[49] For instance, more than a third of consumers would like proof that the company had fixed the issue that led to the data breach, whereas only 8% of security executives would prioritise the provision of this information.[50] In addition, the effectiveness of the mandatory data breach notification scheme could be enhanced if accompanied by other forms of regulation, such as forcing manufacturers to upgrade software when flaws are identified, or requiring users to change default passwords before first using their connected devices.[51]

---

[44] Ingram 2017 op cit.
[45] Deloitte, 2015 'The Deloitte Consumer Review: Consumer data under attack: The growing threat of cyber crime', p5, available: https://www2.deloitte.com/tr/en/pages/risk/articles/consumer-data-under-attack.html
[46] Riedlinger et.al 2019 op cit. p48.
[47] Ibid p21. See also: Burt 2019 op cit.
[48] Houses of Parliament Parliamentary Office of Science and Technology, 2019 op cit., p3.
[49] KPMG Australia, 2019 op cit., p7.
[50] Ibid.
[51] Sivaraman et.al 2017 op cit. p24.

2. Conclusion

ACCAN again thanks the Department for the opportunity to provide a response regarding Australia's forthcoming 2020 Cyber Security Strategy. While we have not offered technical advice nor answered each of the questions raised in the call for views, ACCAN hopes that the preceding insights into the consumer experience will be useful in the development of the new Strategy. We further hope that consumer concerns and experiences will be prioritised within the actions of the new Cyber Security Strategy, and encourage the Department to continue to engage with consumers and their representative bodies to ensure the appropriateness of any such actions.