Law Council
OF AUSTRALIA

Strengthening Australia's cyber security regulations and incentives

Department of Home Affairs

8 September 2021

Telephone +61 2 6246 3788 • *Fax* +61 2 6248 0639
Email mail@lawcouncil.asn.au
GPO Box 1989, Canberra ACT 2601, DX 5719 Canberra
19 Torrens St Braddon ACT 2612
Law Council of Australia Limited ABN 85 005 260 622
www.lawcouncil.asn.au

Table of Contents

About the Law Council of Australia

The Law Council of Australia exists to represent the legal profession at the national level, to speak on behalf of its Constituent Bodies on national issues, and to promote the administration of justice, access to justice and general improvement of the law.

The Law Council advises governments, courts and federal agencies on ways in which the law and the justice system can be improved for the benefit of the community. The Law Council also represents the Australian legal profession overseas, and maintains close relationships with legal professional bodies throughout the world.

The Law Council was established in 1933, and represents 16 Australian State and Territory law societies and bar associations and the Law Firms Australia, which are known collectively as the Council's Constituent Bodies. The Law Council's Constituent Bodies are:

- Australian Capital Territory Bar Association
- Australian Capital Territory Law Society
- Bar Association of Queensland Inc
- Law Institute of Victoria
- Law Society of New South Wales
- Law Society of South Australia
- Law Society of Tasmania
- Law Society Northern Territory
- Law Society of Western Australia
- New South Wales Bar Association
- Northern Territory Bar Association
- Queensland Law Society
- South Australian Bar Association
- Tasmanian Bar
- Law Firms Australia
- The Victorian Bar Inc
- Western Australian Bar Association

Through this representation, the Law Council effectively acts on behalf of more than 60,000 lawyers across Australia.

The Law Council is governed by a board of 23 Directors – one from each of the constituent bodies and six elected Executive members. The Directors meet quarterly to set objectives, policy and priorities for the Law Council. Between the meetings of Directors, policies and governance responsibility for the Law Council is exercised by the elected Executive members, led by the President who normally serves a 12 month term. The Council's six Executive members are nominated and elected by the board of Directors.

Members of the 2021 Executive as at 1 January 2021 are:

- Dr Jacoba Brasch QC, President
- Mr Tass Liveris, President-Elect
- Mr Ross Drinnan, Treasurer
- Mr Luke Murphy, Executive Member
- Mr Greg McIntyre SC, Executive Member
- Ms Caroline Counsel, Executive Member

The Chief Executive Officer of the Law Council is Mr Michael Tidball. The Secretariat serves the Law Council nationally and is based in Canberra.

Acknowledgement

The Law Council is appreciative of the contributions of the following bodies to this submission:

- The Law Society of New South Wales;
- The Law Society of South Australia;
- The Queensland Law Society; and
- The Business Law Section's Corporations Committee, Competition and Consumer Committee, and Privacy Law Committee.

Introduction

1. The Law Council welcomes the opportunity to respond to the Department of Home Affairs' Discussion Paper titled *Strengthening Australia's cyber security regulations and incentives* (**Discussion Paper**). The matters raised in the Discussion Paper are of critical importance, and the Law Council commends the broad ranging and fundamental nature of the issues canvassed.

2. Australia's existing cyber security regulatory and legal frameworks do not adequately protect consumers. Governments and businesses of all kinds use personal information to secure and control access to essential services, often without another authentication layer. This normalises disclosure of such information.

3. On a practical level, many of the current arrangements provide neither market advantage nor incentive for small to medium enterprises to invest in cyber security.[1] However, too much regulation risks further disadvantaging this already under pressure part of the economy.

4. The scope of the challenge cannot be understated. Securing one network and the organisation using it is difficult. Securing a shared digital environment accessed by multiple organisations is even more difficult due to the exponential increase in the size of the attack surface. Current artificial intelligence (**AI**) security investigation systems are promising, but are still considered emergent technology. Further development is required before they can provide sufficient confidence.

5. Unfortunately, in a classic 'arms versus armour' technology race, it is likely that AI enabled attacks will progress as rapidly as AI enabled defences. Even with AI removed from the equation, increasing sophistication and resources available to cybercriminals means that the definition of 'good' or 'adequate' security for many organisations is constantly evolving.

6. The mistaken belief that technology can solve the security challenge is widespread. As Schneier has noted, 'If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology'.[2] Whilst security technology plays an important role, the human interface remains a major vulnerability.

7. Against this context, policy initiatives should avoid the same technology trap. Information security is an organisational and often industry-wide challenge which requires consistent application of 'people, process and technology' levers.

The role of regulatory intervention

Factors preventing adoption of cyber security best practice

8. Improved cyber security can be expensive, and may impede customer convenience and staff productivity. Without a significant incentive to drive action, token efforts are attractive. This is particularly true for smaller or start-up enterprises where a competitor that does not invest in appropriate cyber security may have a price advantage with no short-term market disadvantage.

[1] For example, there is no incentive to minimise the amount of high value personal information retained by a business, to control the distribution of such data in their networks nor to minimise attack surface.
[2] Bruce Schneier, *Secrets & Lies Digital Security in a Networked World* (John Wiley & Sons, 15th Anniversary, 2000).

9. An effective defence depends upon creation of a security culture[3] requiring sustained effort from multiple divisions within the business. In many organisations there is no adequately senior champion to design and drive the necessary activity across multiple departments and functions in the business. Absent a clear understanding of the challenge at both an executive and 'coalface' level, cyber security improvements may be overly focussed on technical defences. If delegated to the IT department, an information security project will - almost by necessity - become focussed on the technical elements of the challenge. Other vital controls, such as policy or training may well be employed, but usually not as effectively as they would be in a more integrated process.

10. Small to medium enterprises (**SMEs**) can also have difficulty knowing where to start. The threat seems remote and intangible. However, purchasing a bespoke risk assessment is expensive and there is often little available guidance for SMEs in mapping an appropriate roadmap to maturity.

Information asymmetries

11. It is difficult for an 'outsider', even a well-informed one, to gauge an organisation's information security maturity without a formal assessment. Information asymmetry is hardwired into purchasing decisions.[4] SMEs and individual purchasers are therefore not always in a position to assess the security cost represented by the cheaper product or service, so market choices will not drive improvement.

12. Without a clear framework in place, organisations may be able to claim high standards without the expense of actually delivering them. In many cases, the cost of information loss will be borne by those who did not have any reasonable opportunity to avoid it.

Weaknesses in the current regulatory framework

Current limitations

13. With the exception of the Australian Consumer Law (**ACL**) provisions,[5] the current regulatory framework does not provide private rights to individuals to take action against bad actors, nor a practical way to recover compensation from a negligent information holder.

14. The current regulatory framework is business/corporation centric and does not anticipate that cyber-attacks originate from individual bad actors who are not businesses or corporations. In particular, the regulatory framework does not give a private right to individuals who are victims of cyber-attacks where the bad actors or defaulting information holders do not fall under the ACL, the *Privacy Act 1988* (Cth) (**Privacy Act**) or the *Corporations Act 2001* (Cth) (**Corporations Act**). This is particularly true in respect of cyber-attacks from individual bad actors hacking computers where no material harm can be established by the victim and existing regulatory frameworks do not expressly anticipate nuisance. This creates a situation where individual bad actors

[3] Loosely defined as a culture in which information security is prioritised, well-crafted policies and procedures support safe data handling, and all network users have specific guidance and consistent support in applying those policies.
[4] The Discussion Paper notes at page 11 that an information asymmetry occurs 'when the sellers of technology products have more information about cyber security than buyers'.
[5] *Competition and Consumer Act 2010* (Cth) sch 2.

are not brought to account in situations where the police refuse to become involved and victims are then left with little or no recourse.[6]

Strengthening governance arrangements

15. To encourage stronger cyber security risk management within organisational decision making, there are two considerations that should be front of mind:

    (a) An impending need for cyber security agility

    As cyber-attacks become increasingly sophisticated, there is an impending need to ensure cyber security practices can be regularly adapted and improved. To facilitate the adoption of new technologies, and to promote Australia's growth as a modern digital economy and a leader in AI (an ambition set out in the Australian Digital Economy Strategy[7] and the AI Action Plan[8]), regulatory settings should provide incentives for Australian organisations to adopt a dynamic and iterative approach to assessment, mitigation and management of cyber security risks, that tracks and responds to emerging threats and vulnerabilities.

    (b) Defining the different roles of actors when managing cyber security risks across the supply chain

    Often security issues arise because points of vulnerability emerge over time through a combination of devices and services, or changes to particular devices or services as used in combination or interaction with other services.

    Mitigation and management of cyber security risks therefore often require organisations to understand whether and how other entities are addressing security risks that arise within a multiparty data handling and processing ecosystem. Cyber security settings of each entity within this multiparty ecosystem may lead to vulnerabilities arising elsewhere in the ecosystem. Security of a particular internet accessible device or service is often dependent upon configurations and other settings made by others in relation to different but interacting devices or services and over time. 'Security' of a particular internet accessible device or service must therefore be assessed over time, and having regard to factors that are often outside the control of the supplier or user of a particular device or service.

    Given the diversity of actors, increased complexity of supply chains for internet accessible devices and services, and the variety of contexts and scenarios of deployment and use, a 'one size fits all' regulatory requirement that a device or service must be 'secure' is unlikely to provide appropriate incentives for entities across a multiparty data handling and processing ecosystem to assess and address evolving cyber security risks.

The value of a voluntary principles-based governance standard

16. The Discussion Paper provides two key options in terms of strengthening governance standards in relation to cyber security. It is, however, not entirely clear whether these governance standards are intended to apply to large companies (with potential

[6] Department of Home Affairs, Strengthening Australia's Cyber Security Regulations and Incentives (Discussion Paper, 2021), p 53.
[7] See, <https://digitaleconomy.pmc.gov.au/>.
[8] See, <www.industry.gov.au/data-and-publications/australias-artificial-intelligence-action-plan>.

attendant accessorial liability for directors) or the directors themselves. The mention of 'if not why not' reporting via the ASX Principles of Corporate Governance suggests the former.

17. One option canvassed is the imposition of a new mandatory governance standard (or legal duty) on directors specifically related to cyber security, which would require companies to achieve compliance within a specific time frame. The other option suggested by the paper is a voluntary principles-based (rather than prescriptive) governance standard, co-designed with the industry and aligned with international standards.

18. The majority of input received by the Law Council from its membership is generally opposed to the introduction of such a mandatory governance standard at this point, however it is noted that the Queensland Law Society (**QLS**) has expressed some support for this proposition, as set out in further detail below.

19. The primary concern with a mandatory standard is that it may be too onerous and costly to comply with. On these matters, the Discussion Paper notes the cumulative impact of a mandatory standard on the level of regulatory burden, and the high costs that such a standard would impose on businesses (which might be passed onto consumers). Directors of companies are already overburdened by regulatory requirements and face potential liability under a myriad of Commonwealth and state laws. The addition of further potential liability is undesirable. The Discussion Paper also notes the potentially difficult interaction with the regulation of cyber security in other jurisdictions and the lack of a regulator with the relevant capacity to develop and administer a mandatory standard.

20. It is important to note that, even without a new mandatory or voluntary governance standard, directors may incur liability for breach of their more general directors' duties. In particular, directors already are obliged by section 180 of the Corporations Act to manage their company with care and diligence - an obligation that may be contravened if they fail to set proper standards of cyber security to be implemented by management for the protection of the company's business. The directors' duty of care and diligence could also be contravened if they fail to take appropriate steps to prevent their company from contravening cyber security laws, via 'stepping stones' liability under section 180 of the Corporations Act.[9]

21. Additionally, if it appears that directors have turned a blind eye to data protection or privacy requirements, the Australian Securities and Investments Commission (**ASIC**) may initiate an investigation which, in serious cases, could lead to proceedings for a pecuniary penalty or compensation order against, or possibly even disqualification of, those directors for failure to comply with their statutory duty of care and diligence.

22. As also alluded to in the Discussion Paper, it is likely that judicial expectations of what a reasonable director might do to oversee the management of cyber risk will rise in light of the increasing awareness of cyber security risks, the increasing number of attacks and the potential damage caused by such incidents. In short, section 180 of the Corporations Act already provides an avenue by which directors could be held liable for failure to discharge their duty of care and diligence in relation to cyber security .

[9] For discussion of stepping stones liability in the context of disclosure, data and cyber security breaches see Rosemary Teele Langford, 'Data Explosion and Stepping Stones' in Andrew Godwin, Pey Woan Lee and Rosemary Teele Langford (eds), *Technology and Corporate Law: How Innovation Shapes Corporate Activity* (Edward Elgar Publishing, August 2021).

23. It is noted that in other circumstances, voluntary standards for banking practices and climate reporting have been effective in providing a benchmark by which stakeholders can hold corporations and their boards to account for failing to comply with such standards.

24. While acknowledging the opposing view of the QLS set out below, the Law Council generally favours the introduction of a voluntary standard. As specifically stated in the Discussion Paper, a voluntary standard could be considered by a court when determining whether failures relating to the oversight of cyber risk constituted a breach of directors' duties. Such a standard should be developed in close consultation with the industry and then subject to broader public consultation.

25. Introducing a designated 'security champion' into the board or senior management structure (an option discussed from paragraph 31 below) could be difficult to implement and even counter-productive. The person designated as 'security champion' could be exposed to a higher standard of care and diligence than other senior officers of the company, an outcome that would create a real disincentive to acceptance of that role. Additionally, those directors and senior executives who are not 'security champions' might come to believe they are not required to consider cyber security except when the topic is specifically raised by the designated person. The Law Council believes these consequences would be undesirable.

26. In the Law Council's view, a voluntary standard for compliance is the most agile and responsive approach to managing cyber security risk through corporate governance and addressing the considerations mentioned above. The National Institute of Standards and Technology (**NIST**) Cybersecurity Framework, an initiative of the United States government, is an example of the practicality and relevance of such a voluntary framework when dynamically managing evolving cyber security risks.

27. The NIST Framework provides cyber security guidance to all sectors and communities in plain English, guiding organisations to consider the appropriate level of cyber risk management for their activities, and assists organisations to prioritise cyber risks in alignment with their goals and resources. The voluntary standard focusses on the identification of critical processes and assets, securing information pathways, maintaining a hardware and software inventory, establishing policies that define cyber security roles and responsibilities, and identifying threats to assets.[10]

28. Likewise, the NIST Framework guides organisations to protect against, detect, respond to and recover from negative cyber security events. This is consistent with option 1 in the Discussion Paper, namely voluntary governance standards for larger businesses.[11] We support the NIST model for cyber security standards for its cost-effectiveness, flexibility, comprehensiveness and wide applicability to different sectors[12] and its international recognition as the basis of the European Commission's 2018 *Directive on Cyber Security*.[13]

---

[10] National Institute of Standards and Technology, 'Cyber Security Framework', Computer Security Resource Center (Web Page, 15 July 2021) <https://csrc.nist.gov/Projects/cybersecurity-framework/nist-cybersecurity-framework-a-quick-start-guide>.

[11] Department of Home Affairs, *Strengthening Australia's Cyber Security Regulations and Incentives* (Discussion Paper, 2021) 21.

[12] National Institute of Standards and Technology, '*Framework for Improving Critical Infrastructure Cybersecurity Version 1.1'* (Report, 16 April 2018) 1 <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>.

[13] Barbara Krumay, Edward WN Bernroider & Roman Walser, '*Evaluation of Cybersecurity Management Controls and Metrics of Critical Infrastructures: A Literature Review Considering the NIST Cybersecurity Framework'* (Conference Paper, Nordic Conference on Secure IT Systems, 28 November 2018); Directive

29. The Law Council notes concern that a voluntary standard may not provide a strong incentive for uptake. For this reason, incentives will be critical to ensuring businesses adopt standards and improve their cyber security. To this end, consideration could be given to the implementation of a trust-mark and industry-led certification to incentivise engagement. Active promotion by government, consumer and industry associations will heighten the credibility of the certification, and its efficacy as an incentive.

Additional views of the Queensland Law Society

30. The QLS has expressed a slightly different view to the above, providing its in-principle preference for mandatory governance standards for larger business within a specific timeframe. The QLS notes that this approach will enable educational institutions in Australia to develop an education framework against a declared standard and support the adoption and implementation of those standards across the economy in a sector appropriate way.

31. To support this proposed approach, the QLS has proposed that all Privacy Act regulated entities could have at least one board member or senior executive with an approved cyber-governance qualification. Ensuring senior level engagement is a low cost first steps element of a mandatory cyber risk management framework. This regulatory intervention would be relatively inexpensive for both government and business.

32. The QLS notes that these qualifications need not be onerous and could be effectively provided online in a few weeks part-time. In addition to mandatory training for the senior leadership of larger organisations, subsidised or free training aimed at the owners or senior managers of smaller enterprises should be available and encouraged. This is a very specific audience, so the content should be appropriately tailored and differentiated from 'awareness' material which is provided to coalface staff. Further, whilst these may initially be targeted towards larger businesses, in the view of the QLS, they should be available to assist entities of all sizes. In doing so, the QLS raise issues related to the scope of the Privacy Act and in particular the application of the small business exemption[14] and potentially the employee records exemptions[15].

33. The QLS further points out that governance training may be best delivered as an online course hosted/delivered by the Australian government. Contributors could include universities, professional associations and cyber risk consultancy practices. Delivery of this training by government would assist in providing ease of access, consistency and remove any cost barriers for smaller businesses seeking to access the content.

34. The objective of the training would be to improve the understanding of cyber risk governance, the holistic control measures available and how change management should be approached, not to create a technical expert. In the view of the QLS, a certificate of competency could also be issued to assist with content engagement.

35. The QLS notes that upon course completion, access should be facilitated to a self-paced online security maturity assessment which generates a report that is easily consumable and shows the users maturity as against industry best practice and the prioritisation of remedial steps.

36. The QLS points out that the first task the 'security champions' may face will be to explain the issues to their colleagues. A suite of credible materials aimed at a non-technical audience articulating the risks and consequences of underinvestment should be

(EU) 2016/1148 of the European Parliament And Of The Council Of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union [2016] OJ L 194/1.

[14] *Privacy Act 1988* (Cth), Section 6D.

[15] Ibid, Section 7B.

provided by the Australian Cyber Security Centre to assist in this challenge. Collaboration with industry associations and peak bodies to modify the toolbox contents for their target audience would be valuable.

37. The QLS further takes the view that Australian Privacy Principle (**APP**) 11 could include a mechanism for industry associations and peak bodies to negotiate an appropriate standard articulating 'reasonable steps'. This should then be a safe harbour from a regulatory perspective and be persuasive (but not definitive) in determining civil liability based on negligence.

38. The QLS acknowledges that it will be difficult to develop a code with such wide application, and therefore submits that a maturity model scaling different requirements to different sized business is appropriate. In the view of the QLS, the standard should not specify the content of mandatory controls to avoid becoming a dead hand on what must be a fast-evolving risk mitigation environment.

39. It is noted, however, that caution should be exercised to ensure that companies are not subjected to both liability through a breach of an APP and subject to consumer redress claims where there has been a failure to take reasonable steps to ensure only authorised access to personal information occurs.

Application to the legal profession

40. Law firms and legal practices represent an attractive target for cybercriminals, and the Law Council recognises that cyber security needs to be something lawyers normalise as part of their everyday working lives. Lawyers have a professional duty to protect their clients' information. While there are some slight jurisdictional differences, the general duty is much the same throughout Australia. The issue of client confidentiality is now well-accepted as being threatened by inadequate cyber security arrangements.

41. To this end, the Law Council, with assistance from its Constituent Bodies developed the *Cyber Precedent* suite of resources to assist the legal profession to actively protect itself from cyber-attacks.[16]

42. Many of the Law Council's Constituent Bodies have also been active in publicising information for practitioners about cyber security issues and related preventive steps through information sharing and continuing professional development programs.

43. For example, the Law Society of South Australia (**LSSA**) has advised that it has entered into a licensing agreement with Lexon, the Queensland professional indemnity insurer, to provide a suite of helpful documents regarding cyber security which are available to all South Australian insured practitioners via the Society's website.

44. The LSSA further advises that it continues to emphasise preventative strategies which should be taken by lawyers and law firms, are based in large part on the Federal Government's 'Essential 8' things that can be done to minimise cyber security incidents.[17]

45. The LSSA intends to continue its focus on cyber security education into the future, and through its Professional Indemnity Insurance Scheme is looking at an additional insurance solution which may in the future be available to legal practitioners in South Australia, and depending on the nature of the available policy, may have certain

[16] See, <http://lca.lawcouncil.asn.au/lawcouncil/cyber-precedent-essentials>.
[17] See, <https://www.cyber.gov.au/acsc/view-all-content/essential-eight>.

minimum standards (likely to be based largely on the Essential 8) which practitioners will be required to meet before that insurance is made available.

46. In relation to cyber insurance generally, the LSSA notes that market forces drive the position with respect to the provision of insurance and the scope of cover. At the moment, the Society understands the market is substantially hardening with insurance capacity, scope of cover and aggregate limits being more limited. This reflects a number of the matters identified in the Discussion Paper with respect to increased cyber risks and reinforces the importance of a greater focus on cyber security measures, including increased education about those risks.

Support for SMEs

47. The development of a voluntary health check for small businesses, in line with the recommendations in Chapter 9 of the Discussion Paper, is supported in principle. A collaboration with the insurance industry to assist 'health checked' small businesses to obtain comprehensive, affordable cyber risk insurance (in line with a successful model in the UK)[18] could also be beneficial.

48. Similarly, liability caps and safe harbour for compliant businesses (similar to the Professional Standards Scheme) should be considered.

49. For the most part, there is support for a voluntary risk management framework for smaller businesses as opposed to mandating a code, but the QLS has noted that one notable exception could be a business which chooses to hold High Value Personal Information (**HVPI**), as outlined further below. As noted above this needs to be considered as part of the broader review of the Privacy Act and specifically the exemptions and related definitions that may overlap with the new concept of HVPI[19].

50. Simple and voluntary governance standards designed to educate SMEs could also be beneficial and avoid the increased costs of compliance with a mandatory framework.

Consumer guarantees and recourse

Application of the consumer guarantees

51. The Competition and Consumer Committee of the Law Council's Business Law Section (**the Committee)** considers that existing provisions in the ACL, namely the consumer guarantees, are sufficient in addressing the concerns raised in the Discussion Paper.

52. The Committee notes that consumer guarantees provide a series of non-excludable statutory guarantees that apply to goods and services supplied to consumers. The definitions of 'goods' and 'services' in the ACL are drafted broadly such that they capture digital products and services. For example, the definition of 'goods' in the ACL expressly includes 'computer software'. The Australian Competition and Consumer Commission (**ACCC**) has successfully taken action against suppliers in relation to representations made about digital products and services, such as online games.

53. The consumer guarantees regime addresses a broad range of deficiencies, including those that arise from the use of new technologies and vulnerabilities that those

[18] UK National Cyber Security Centre, <https:// www.ncsc.gov.uk/collection/small-business-guide>.
[19] For example, the definition of *sensitive information* or *identification information* in section 6 of the Privacy Act.

technologies may face from cyber-attacks. The consumer guarantees provide, relevantly, that:

- goods supplied to a consumer must be of acceptable quality and be fit for any disclosed purpose; and
- services supplied to a consumer must be rendered with due care and skill and be fit for purpose.

54. The Committee considers that the consumer guarantees are likely to provide adequate protection against cyber security risks. In the Committee's view, the consumer guarantees require suppliers to ensure that digital products and services supplied to consumers offer a sufficient level of protection against cyber security threats.

55. A consumer is entitled to certain remedies from the supplier where the consumer guarantees have not been complied with, regardless of who manufactured the parts responsible for the failure. The consumer may also recover compensation for any reasonably foreseeable loss or damage suffered due to the supplier's failure to comply with the consumer guarantees. Where a supplier is liable to a consumer for breach of the consumer guarantees, the supplier has a right of indemnity against the manufacturer. In some circumstances, remedies can be sought directly from the manufacturer by the consumer.

56. The Committee considers that the operation of the consumer guarantees, as described above, provides proper incentives to suppliers and manufacturers to take reasonable steps to invest in cyber security.

Access to justice

57. A well-functioning consumer redress system is essential for the effective operation of the consumer guarantees as they apply to digital products and services.

58. The Law Council notes that there are a number of avenues through which consumers can seek redress for a breach of the consumer guarantees. Consumers have recourse to consumer tribunals as well as courts. They can also seek assistance from the ACCC and state and territory regulators that can take action where the matter is of significant public interest or involves substantial consumer detriment. The ACCC, in particular, has a demonstrated track record of taking enforcement action in respect of systemic breaches of consumer laws, including in response to complaints received from consumers.

59. The Law Council is, however, supportive of the introduction of alternative dispute resolution mechanisms to better resolve complaints about the consumer guarantees, such as compulsory conciliation or direction powers. This would improve the practical functioning of the consumer guarantees by making it easier for consumers to obtain a remedy. In this regard, the South Australian compulsory conciliation scheme and the power of the New South Wales Commissioner for Fair Trading to issue consumer guarantee directions may be useful models to apply to other jurisdictions.

60. However, the Law Council submits that such regimes should not be introduced more broadly without a detailed cost/benefit analysis of the operation of those regimes to date, and appropriate community and industry consultation.

Penalties for failing to provide a consumer guarantee

61. The Committee is not supportive of the introduction of a civil prohibition for failing to provide a consumer guarantee remedy in the ACL, particularly if it is attached to significant penalties.

62. As noted above and explained in further detail below, there are already robust mechanisms under the ACL to enforce compliance with the consumer guarantees, and the introduction of this new civil prohibition is considered unnecessary.

63. Furthermore, it would not be the appropriate regulatory response to address concerns about non-compliance with the consumer guarantees given the complexities associated with determining whether there has been a breach of the consumer guarantees as well as the remedies available for breach of the consumer guarantees.

Existing enforcement mechanisms available

64. The ACL prohibits persons from making false or misleading representations in connection with the supply, promotion or use of goods or services. This prevents suppliers from misleading consumers about their rights under the consumer guarantees, including their right to remedy for non-compliance with the consumer guarantees. A contravention of this prohibition attracts significant civil and criminal penalties.

65. The ACCC has had considerable success in holding suppliers (including suppliers of digital products and services) accountable for misleading consumers about their consumer guarantee rights through issuing infringement notices, taking administrative action (e.g., court-enforceable undertakings), and via court proceedings. This demonstrates that the current regime is working, and further enforcement mechanisms are not required.

Complexities associated with determining a breach and appropriate remedies

66. Prohibitions which carry a penalty must be sufficiently certain to enable businesses to know, with a high level of certainty, what conduct will expose them to a financial penalty. The Law Council's concern is that assessing a consumer's entitlements under the consumer guarantees requires a complex and fact-based analysis.

67. Firstly, reasonable minds may differ as to whether there has been a breach of the consumer guarantees. This is particularly so in relation to the consumer guarantee as to acceptable quality which involves assessments of a 'reasonable consumer's' expectations as to the acceptability of the good, its durability and safety (which may vary based on the value and nature of the relevant goods).

68. Secondly, the remedies to which consumers are entitled for non-compliance with the consumer guarantees also requires a case-by-case analysis. The available remedies for failure to comply with the consumer guarantees depends on whether the failure is considered 'major' or 'non-major'. The distinction between a 'major' and a 'non-major' failure can be difficult to determine.

69. However, the definition of a major failure in the ACL is imprecise and frequently unhelpful. For example, a major failure in respect of goods or services is defined as including one where a reasonable consumer would not have acquired the goods or services had the consumer been fully acquainted with the nature and extent of the failure. While this limb technically sets a minimum threshold for the type of faults which would amount to a major fault, it is arguable that a reasonable consumer would rarely,

if ever, acquire new goods or services if he or she were aware that there was even one minor failure; at least not without some form of compensation.

70. The Law Council considers that a more appropriate response to the concerns raised in the Discussion Paper is additional regulatory guidance, and targeted regulatory engagement with suppliers and manufacturers of digital products and services. The ACCC and State regulators would be well placed to do this. For example, the ACCC has published detailed guidance on its view of the application of the consumer guarantees to the supply of motor vehicles.

Additional views of the Queensland Law Society

71. While noting the above comments, the QLS holds the view that the ACL does not provide sufficient redress for individuals. In particular, the QLS is of the view that:

- The ACL does not specifically contain actions for breaches of a computer system. Rather a victim would need to rely on general provisions such as misleading and deceptive conduct in the course of trade. If the event has occurred outside the course of trade those provisions are of no utility to the victim.
- The ACL provides a right to apply to a court for damages for loss or damage arising from a contravention of the ACL. Therefore, for an applicant to succeed under the ACL it must establish loss or damage which has arisen as a result of the contravening conduct. This is more difficult in the cyber security setting as, firstly, damage must be anticipated (and able to be articulated) or suffered before taking action. Secondly, there is an evidentiary burden to establish that the loss or damage occurred due to the breach.
- The breach may be an identity theft and it can be very difficult to identify the source of the breach, particularly if the person is the subject of multiple breaches.

72. The QLS has submitted that there needs to be specific legislation to ensure that Courts exercising civil jurisdiction can make orders protecting the confidentiality and property rights of parties adversely affected by cyber intrusion.

73. The QLS has recommended that consideration should be given to the following to improve coverage and enforcement of cyber security requirements:

- Amendments to the ACL to ensure that:
  - software and specifically cyber security is a good or service;
  - statutory guarantees are extended to provide broader coverage including in business to business sales; and
  - consumers have clear rights of redress against suppliers of software or services that do not meet regulatory standards.

74. Other suggestions for reform put forward by the QLS include:

- The current regulatory framework should be extended to include a breach of privacy in a cyber/computer setting. Including for example, to require information holders to take positive steps to preserve confidentiality, not just refrain from disclosure (in the same way as agencies, organisations and businesses covered by the Privacy Act are obliged to deal with personal information noting also that attacks go beyond what is 'personal information').

- The introduction of *sui generis* legislation to.
  - provide a private right to individuals who are victims of unauthorised access to networks or data; and
  - give individuals a private right to take action for cyber security incidents where the bad actor falls outside the scope of the existing regulatory frameworks. These provisions should include appropriate restraints where breach of Court order constitutes contempt.

Minimum standards for personal information

The merits of a cyber security code under the Privacy Act

75. The QLS has advised the Law Council of its view that there should be a cyber security code applicable to entities regulated by the Privacy Act and recommends further consideration of the appropriateness of the Privacy Act's definition of Personal Information. This might include for example, a further classification of Personal Information be added to the Privacy Act, namely HVPI.

76. The QLS notes that examples of HVPI could include:

- soft copies of identification documents;
- medical and privileged legal information;
- financial records, including transaction history and account details, credit card numbers;
- information which may place an individual at risk of harm if released.
- information which is likely to cause high levels of distress or economic loss if released;
- information which would reasonably facilitate identity theft or crime; and
- high volumes of personal information that does not meet the other criteria.

77. QLS submits that whilst requirements could vary between businesses based on size, all HPVI requires protection. The QLS asserts that the Office of the Australian Information Commissioner should be sufficiently resourced to assist small businesses to understand their obligations including to provide guidance materials.

78. As noted above, the Law Council considers these matters go to the scope and structure of the Privacy Act and will need to be considered as part of the pending review of the Privacy Act.

Attributes of any cyber security code

79. In considering the benefits of a cyber security code applicable to entities regulated by the Privacy Act, the QLS suggests that the best starting point for technical controls as a mandatory code would use the UK's Cyber Essentials for smaller entities,[20] and the Australian Essential 8 for larger ones.[21]

80. In addition to the technical controls specified in the Essential 8, the QLS notes that additional risk mitigation dimensions would be required including:

[20] See <www.ncsc.gov.uk/cyberessentials/overview>.
[21] Australian Cyber Security Centre – Essential 8, <www.cyber.gov.au/acsc/view-all-content/essential-eight>.

- policy adoption in such areas as access credentials, encryption, shadow IT, and appropriate locations of sensitive data;
- physical security measures;
- pre-recruitment checks; and
- induction and refresher training.

81. The QLS highlights as an example of an entry level mandatory code the security requirements applicable to all electronic conveyancing subscribers by the Australian Registrars' National Electronic Conveyancing Council (**ARNECC**) Model Participation Rules. It is notable in that recruiting, background checks and training are all emphasised in addition to technical defences.

82. The QLS points to a more ambitious model in the Payment Card Industry Data framework. A notable feature of that approach is that businesses have an opportunity to avoid onerous security restrictions if they choose not to hold the high value data themselves. By way of illustration, in the example of personal data typically provided to an agent as part of a rental application, the agent could obtain an identification verification certificate from a third-party provider rather than demanding copies of driver's license and passport. Alternatively, the franchisor could supply a secure data lodgement portal to avoid transmission and storage of the data using email accounts.

83. By definition, a generic code will struggle to be equally useful across all sectors of the economy. What is appropriate for, say, a real estate letting agent would be too onerous for a real estate sales agent. QLS submits that industries should be given scope to negotiate a more appropriate code through their peak bodies or member associations. To avoid a race to the bottom, the approval agency should adopt a 'no consumer detriment' test. Again, these matters would benefit from consideration as part of the pending review of the Privacy Act. For example, there may be benefits of articulating safe harbours as applicable and notions of adequacy or equivalency that apply in other data protection or related regimes.

The scope of any cyber security code

84. The QLS notes that the trigger for applicability of any cyber security code should be the potential for damage posed by the loss of the data rather than the size or sector of the entity holding it.

Standards for smart devices

85. Although Chapter 6 of the Discussion Paper does not directly concern itself with raising public awareness, it will have an impact on how connected things are perceived by the public. A key difficulty in solving the issues raised in the Discussion Paper is the interdependence of the technology and the connectivity of smart devices.

86. When an IT product is publicly released there is often an innate trust that somehow a regulatory authority has assessed the product to ensure that it is safe to use.[22] However, this is not always the case. Only critical systems are assessed, and even then, only against industry standards. As Scott has noted, 'Governments do not and cannot regulate everything. … A regulatory regime is the aggregation of the activities of those whose actions shape behaviour within a particular set of activities'.[23]

[22] McCullagh, A., 'E-commerce – A matter of Trust', Australian Computer Society Workshop at the Australian National University, 1998, ACS publication.
[23] Scott, C., 'Regulating Everything', UCD Geary Institute – Discussion Paper Series 2008.

87. Government needs to provide a cyber security framework which is affordable and offers confidence to the public as a protective measure. Each iteration could involve a feedback loop so that government or the regulatory agency administering the regulatory regime is able to make adjustments to improve the desired outcomes. It is likely that this adoption will, as with most cultural change programs, encounter some resistance. The Law Council has reservations that a mandatory approach through the implementation of penalties will be effective given that so many 'Interest of Things (**IoT**) devices are imported by the end user. A better approach may be an incentive scheme. This is discussed more fully below.

Interconnection of Devices

88. The interconnected environment has developed over the last 15 years to become pervasive. On 29 June 2007 Apple released the iPhone 1 (Model number A1203), which was the first consumer released smart phone. As of November 2020, there were 20.1 million smart devices (smart phones and tablets combined) deployed in Australia.[24] This number is expected to increase to 21.5 million devices by 2025.[25] At the same time, the development of Wi-Fi was taking hold in both the consumer and non-consumer markets (both government and industrial settings). There has in the last 12 months been numerous publications that have attempted to estimate the global number of interconnected things and the economic benefits from IoT deployment.[26] The numbers range from 25 billion interconnected devices to 41.1 billion interconnected devices by 2025.[27]

89. As the internet has evolved over the years, new laws have been introduced and important steps taken towards international harmonisation structures. With the proliferation of interconnected devices, new regulations will need to be created. No one can prevent a cyber-attack nor is it possible to eliminate these attacks entirely. However, it is possible to reduce the incidence of cyber-attacks and to reduce the risk of a successful cyber-attack. The implementation of cyber security technology is clearly an important factor but the more complex question is how far should a technology provider go to ensure that their technology is safe and fit for purpose? This requires consideration of what the terms "safe" and "fit for purpose" look like in this context.

90. For example, a CCTV device that allows its owner to monitor their premises via their smart phone has a simple function, but should the manufacturer also be required to ensure their device is not subject to trivial cyber-attacks? Where a CCTV device is basically insecure and vulnerable to less sophisticated cyber-attacks but it is doing what it is expected to do, can it be said to be safe or fit for purpose? That is, it is activated through motion sensors, and captures motion as and when it occurs. At the same time, there have been incidents where a CCTV device has been subject to a successful cyber-attack and the images are not only being able to be seen by the rightful owner but are being auctioned in real time via the dark web to local criminals so that the criminals can burgle the relevant home/premises.[28] The local criminals are obtaining vital information about the premises by knowing when the premises are likely to be vacant.[29]

---

[24] Statista, *Number of smartphone users in Australia in 2017 with a forecast until 2025* (September 2020) <https://ww.statista.com/statistics/467753/forecast-of-smartphone-users-in-australia>.
[25] Ibid.
[26] McKinsey Report on IoT, <www.mckinsey.com/mgi/overview/in-the-news/by-2025-internet-of-things-applications-could-have-11-trillion-impact>.
[27] Ibid.
[28] Hackers successfully attacked an Iranian Prison's CCTV installation showing torture being carried out <www.securitynewspaper.com/2021/08/23/hackers-break-into-irans-famous-prison-and-leaks-cctv-footage-for-tortures/>, BBC news: Hackers attack 150,000 IoT cameras installed in UK schools <https:// www.bbc.com/news/technology-56342525>.
[29] See, <https:// cisomag.eccouncil.org/10-iot-security-incidents-that-make-you-feel-less-secure/>.

91. The issue for base protection is addressed in ETSI 303645 by requiring IoT manufacturers not release an IoT device as a set and forget product. Manufacturers should, as noted in ETSI 303645, be required to monitor any security vulnerabilities later identified and be able to patch the device through a firmware update. This requirement is explored in more detail below.

Possible government intervention

92. A major difficulty for the Australian market is that Australia only has a very small IT sector compared to other jurisdictions. This makes it very difficult for any entity whether private enterprise or government to verify the security structure of the technology. Whilst there are case tools in existence that can assist in vulnerability testing, they are not foolproof. For example, it is possible to test software applications against *known* vulnerabilities such as a Structured Query Language injection or stack overflow attacks. However, there are new attack routes arising on a daily basis and some are not directed at the deployment of software but are directed at the hardware itself. An example of this was the Stuxnet worm.[30]

93. One challenge in regulating IoT devices is that they are not only attractive to low level criminals with commercial objectives but as a point of entry for state sponsored hackers targeting critical infrastructure (CI).Such attacks are likely to emanate via an IoT device which, on the surface, appears not to be connected to any critical device but through multiple interconnections or supply chain relationships can attach itself to a CI device and cause substantial economic and social damage.

94. Whilst the threats posed by technology are a significant issue, it is also important to acknowledge the benefits that technology has brought and brings. The Discussion Paper notes the economic and societal costs of cyber security incidents. In considering government interventions, technology as a key economic growth factor should also be recognised. Government reforms should be cautious of steps which remove the benefits of and/or discourage people from adopting technology.

95. To respond to the complexities in the smart devices environment, the government might consider the following areas.

Self-certifying environments

96. From a regulatory position it is open for the government to require any organisation to publicly certify that the IoT device being deployed has been subject to a security test which corresponds to an acceptable IT security standard. By way of example, ISO 15408 (Common Criteria Target of Evaluation) is a security assessment and EAL 3 (Evaluated Assessment Level) or above may be appropriate.

97. Mandating manufacturers and importers of IoT devices to undertake such testing either internally or via a NATA assessment could improve the security of the IoT environment. However, it will be only one factor in a multifactorial solution.

Taxation incentives

98. Consideration could be given to taxation incentives for manufacturers and/or importers to have appropriate security prebuilt into all IoT devices. The nature of and amount associated with the taxation incentive could be costed and set against the cost of the

[30] See Eric D. Knapp, Joel Thomas Langill, 'Industrial Cyber Security History and Trends', in *Industrial Network Security* (Second Edition), 2015.

realistic risk of a successful attack.[31] Consequently, some economic analysis is required to ensure a balancing of the costs.

Government contracting and supply chain management

99. The Australian Government is by far the largest single IT purchaser in Australia. Therefore the government could have a significant influence on manufacturers and importers to implement appropriate IT security technology within their deployed devices. This approach mirrors the US position.[32] As the NIST prepares standards as required by that legislation, manufacturers will have a significant incentive to improve security, at least for higher end devices. Australia can benefit from this approach, ideally by adopting the same standards if they are appropriate.

Standards compliance

100. It is submitted that a prescriptive mandatory security standard regime for IoT products should not be introduced at this stage. That may change at some time in the future when a consensus as to appropriate minimum requirements emerge. Until then, a less prescriptive regulatory regime may be appropriate.

101. By way of example, the California IoT law requires manufacturers of connected devices 'to equip the device with a reasonable security feature or features that are appropriate to the nature and function of the device, appropriate to the information it may collect, contain, or transmit, and designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure, as specified.'[33]

102. According to the Californian Department of Justice (**Cal DoJ**) the minimum security required under the law would be the 18 security controls promulgated in the CIS Critical Security Controls for Effective Cyber Defence.[34] This determination does not mandate that such security controls are absolutely required but the Cal DoJ may determine that such failure is evidence to be considered on whether to prosecute an organisation for a failure in the security of the device.[35] Any failure to meet a particular security framework could also be considered by a court in an IoT security failure case.

103. Possible standards adoptions which could be considered is the EU's ETSI (EN) 303645 which details the '*Cyber Security for Consumer Internet of Things: Baseline Requirements'*.[36] The shortfall with this approach is that by concentrating on consumer protection the result is a piecemeal position which is counterintuitive to the structure of IoT. It will not be possible to segregate the IoT environment between CI components from consumer products. For example, an internet enabled fridge may be positioned in a hospital or in the canteen of an energy manufacturer. If that fridge is compromised to somehow connect to the main-net of the hospital or energy manufacturer then problems could arise.

104. A holistic approach will need to be developed to ensure certain security elements do fall through the cracks causing major problems. Concerns around privacy should not drive

---

[31] For example, if the tax incentive costs the government from a revenue perspective $500 million but the risk of not incentivising commerce could result in a $2billion cost then the benefit of $500 million cost could be justified.
[32] Internet of Things Cybersecurity Improvement Act of 2020 or the IoT Cybersecurity Improvement Act of 2020.
[33] Californian Law: SB-327 Information privacy: connected devices <https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327>.
[34] Centre for Internet Security (CIS), Controls https:// www.cisecurity.org/controls/
[35] See <https:// medium.com/golden-data/california-iot-law-ac91255c8282>.
[36] See <https:// www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.00_30/en_303645v020100v.pdf>.

the security solution. Whilst privacy is obviously important, IT security is much bigger than just privacy.

Responsible disclosure policies

105. The Law Council notes that there may be scope for the creation of a template ethical disclosure policy and payment of bug bounties, citing reports from its membership of good faith reports being met with threats of litigation.

106. One avenue might be a protected channel for security researchers to report concerns to the OAIC. This would give the OAIC the opportunity (but not the obligation) to assess the level of risk and encourage action, and also to take the warning into account when considering subsequent regulatory action.

Health checks for small businesses

Merits of a cyber security health check program

107. It is considered that a cyber security health check program would assist in both awareness and education for consumers and SMEs. The health check could incorporate training and/or accreditation for individuals and businesses to be delivered in a similar manner to the roles/responsibilities of Work Health and Safety and Privacy Officers.

108. Organisations would also benefit from receiving guidance on, and exposure to, best practice. There would be benefit from providing specific actionable steps they can take in their position and/or circumstances. However, a tension will arise where 'healthy' is defined too narrowly and the specific requirements to achieve it are prescribed in a manner that some organisations may tend to see reaching that threshold as sufficient/all boxes ticked and not seek to continuously improve, prepare and respond to changes in the cyber threat environment and in their business.

109. A cyber security health check program can only improve Australia's cyber security if it is adopted by a substantial number of organisations and individuals. In addition, a penetration or success goal should be set and supported by the long-term promotion of the program.

Encouragement for SMEs

110. The United Kingdom experience seems to suggest success with overall general awareness but very low levels of participation (perhaps as low as 1 percent).[37] Noting this challenge, participation can be encouraged in a number of ways:

    - firstly, by promoting the benefits of dealing with a business that displays the 'Trust Mark', by educating SME operators on the importance of meeting certain standards of cyber security, and by making the self-assessment process as efficient as possible;

[37] 'Since the scheme launched in 2014, the NCSC has helped to protect over 60,000 UK businesses from the most common cyber threats':
<www.ncsc.gov.uk/news/new-tool-to-help-achieve-cyber-essentials-certification>;
'At the start of 2020 there were 5.94 million small businesses (with 0 to 49 employees), 99.3% of the total business [in the UK]': <https://www.fsb.org.uk/uk-small-business-statistics.html> [60k/6 mil = 1%].
'This statistic displays the share of businesses that were aware of the Cyber Essentials scheme in the United Kingdom (UK) in 2020, by size of business. A total of 13 percent of all UK respondents were aware of the Cyber Essentials scheme' <www.statista.com/statistics/586565/cyber-essentials-scheme-awareness-by-united-kingdom-uk-businesses/>.

- secondly, by giving SMEs with the 'Trust Mark' some appropriate benefits or recognition when tendering for government work; and
- thirdly, by considering some form of recognition that an SME with the 'Trust Mark' has acted "reasonably" when responding / defending any claims.

111. Health checks, if adopted, should incentivise regular reviews – say, annual or whenever a key change occurs in the business. For example, organisations prepare annual budgets, and annual reports. Similarly, organisations should put cyber on the owners/managers/leader's agenda and position description and have regular discussion about their current and target level for cyber health. A public register of certified organisations would also build trust in the program.

112. Organisations of all sizes and capabilities should be able to assess (in their own context) their current 'cyber health' position/maturity, and plan for how they would move to a higher rung of cyber preparedness and capability in collaboration with people, technology, process and culture. A health check tier / ladder-rung approach to cyber security may assist in this self and ongoing assessment process.

Other issues

Consumer education regarding advertising standards

113. To better protect consumers and businesses, advertised products need to have clear scopes of application. For example, Law Council members report that current advertising approaches mean that consumers often believe that if they use a Virtual Private Network they are protected from viruses and that the Internet Service Provider protects them from viruses.

114. Minimum standards of advertising could be developed to address issues of scaremongering, puffery and promises of results with respect to cyber security products.