The Australian Industry Group

Submission to the 2020 Australian Government Cyber Security Strategy Discussion Paper

T 1300 55 66 77 W aigroup.com.au E info@aigroup.com.au

Contents

About Australian Industry Group

The Australian Industry Group (Ai Group) is a peak national industry association representing and connecting thousands of employers across Australia. We represent the interests of more than 60,000 businesses employing more than 1 million staff and we promote industry development, jobs growth and stronger Australian communities. Our members are private sector employers large and small, with common interests in more competitive businesses and a stronger economic environment. Ai Group members have access to specialist workplace advice and services and to policy leaders and business networks. We connect businesses and our members value Ai Group's expertise and ability to contribute to and influence government policy in areas such as industry policy, workplace relations, education and training, energy, trade, taxation and regulation.

1. Introduction

The Australian Industry Group (Ai Group) welcomes the opportunity to make a submission on the Australian Government's 2020 Cyber Security Strategy Discussion Paper.

Strong cyber secure and resilient businesses are central to customer trust. This includes protecting data privacy, competitiveness, the strength of our economy and the reliability of our infrastructure. While in many ways diverse, business sectors have a common and collective interest to be cyber secure. It is a critical time for improved collaboration between governments and businesses. The 2020 Cyber Security Strategy has an opportunity to enable this.

When the Government released its revised National Cyber Security Strategy in 2016 (2016 Strategy), we saw this as an opportunity to strengthen cooperation between government, industry and other bodies to address both cyber security threats and promote innovation. This Strategy outlined a number of positive initiatives aimed to address the challenges with cyber security.

While positive steps have been made to implement this 2016 Strategy, there are areas that still require further improvement to ensure the spirit of the 2016 Strategy continues in the 2020 Strategy. We discuss these areas in this submission.

Since the 2016 Strategy, we have seen new significant data privacy legislations commence including the Australian Notifiable Data Breaches (NDB) Scheme, European Union General Data Protection Regulation (EU GDPR) and Australian Consumer Data Right (CDR), as well as the controversial *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) (TOLA Act).

Cyber security threats also continue to grow and evolve as a risk management issue for many organisations and their boardrooms, with news about data breaches and cyber security attacks becoming more mainstream. If left unchecked, these can diminish corporate trust and reputation, business and consumer confidence, as well as disrupting business operations and provision of services. And in light of growing public awareness and scrutiny about data privacy and rights, it is important organisations ensure they are adequately meeting public expectations and level of trust. These threats are further compounded as organisations become more digitalised and connected through the internet.

Only a few years ago "digitalisation" seemed like a discussion by and for technology companies. That conversation now extends to businesses well beyond the technology sector. More and more organisations are participating in the Fourth Industrial Revolution (or Industry 4.0) – a transformation of business models driven by connected devices, data analytics and other technologies, comparable in impact to the adoption of steam, electricity, telephony, railways, mass production, automobiles and computers. Business engagement with the current upheaval is growing, maturing and moving well beyond hype and theory. While this presents an important opportunity to boost economic growth, it also has the potential to open up organisations and individuals to new cyber security threats if not managed appropriately.

Therefore, cyber security has become a fundamental risk management requirement for many organisations, as well as the community, as they transition towards or within the Fourth Industrial Revolution. Government has an important leadership role to play, which includes assisting organisations and the community to be fully cyber aware and respond to cyber security incidents to ensure that potential inhibitors to our economic growth are mitigated.

Despite business calls for improved collaboration in line with the spirit of the 2016 Strategy, there have been growing business and broader community concerns with recent Federal Government knee-jerk policy responses under the catch-all umbrella of national security. The rushed development and passage in late 2018 of the TOLA Act, despite widespread business and community objections, poses serious risks to Australians' cyber security and the reputation of

Australian businesses that sell digitally-enabled products and services. Substantial amendments are needed as soon as possible to clarify the Act and limit its impact in the areas of greatest risk.

In addition to outstanding amendments required to the TOLA Act, the Federal Government separately rushed and passed the *Sharing of Abhorrent Violent Material Amendment Act 2019* (Cth) (also known as the AVM Act) through the Parliament in April this year. The community expects protection against extremist violence and discretion from all media in dealing with imagery of that violence. However, the legislation needs to be improved upon to better address community concerns, without unnecessarily impinging on fundamental existing rights and freedoms, and other unintended consequences.

Ai Group continues to support the opportunity for better collaboration with Government to develop a practical and workable solution to address cyber security incidents in an agile and constructive way, and to encourage greater innovation. There are real opportunities for Government to put this into practice.

In this submission, Ai Group addresses the bulk of the questions raised in the Government's Discussion Paper, presenting our research and members' views. The case is clear: Australia does need an updated national Cyber Security Strategy to organise and judge public policy action, to ensure we are doing all we should to lift capability across the economy and seize the digital opportunity. Government cannot and should not do everything, but it has great responsibilities as the developer of critical infrastructure, the guardian of public order, the funder of education and much research, and an influential source of advice and validation. The Government should develop, promulgate and regularly update its Cyber Security Strategy to ensure those responsibilities are faithfully discharged. There is a real chance to lift Australia's performance, to lasting social and economic benefit. We should make the most of it.

Should you be interested in discussing our submission further, please contact our Digital Capability and Policy Lead Charles Hoang ([redacted]).

2. Cyber security threats

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

Businesses and other organisations are exposed to a broad range of different cyber security threats, motivated for different reasons e.g. criminal, industrial espionage, national security (e.g. State-sponsored) and social hacktivism. Arguably, these threats are influenced by the industry and nature of the work of the organisation. It is important that Government takes a multipronged approach to tackling these different types of threats and support organisations to become more secure and resilient. This in turn will help to protect the community against such threats.

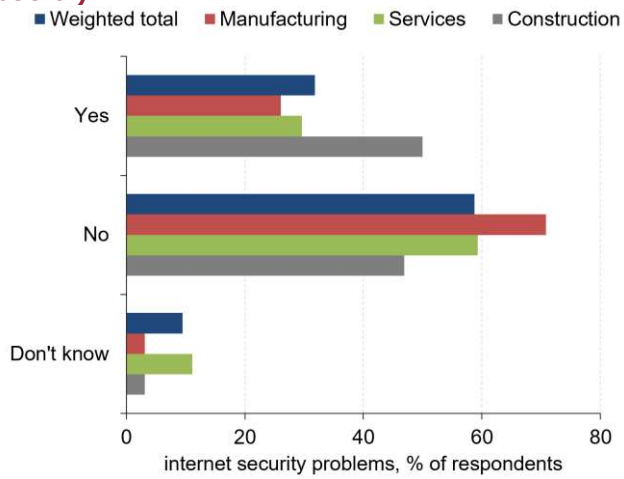
Below we discuss further the types of cyber security threats that we have found in our own research as well as from other sources. These are threats where Government can further assist businesses and the community.

2.1 Cyber security threats

In Ai Group's *CEO Survey of Business Prospects 2019*, we explored business experiences with

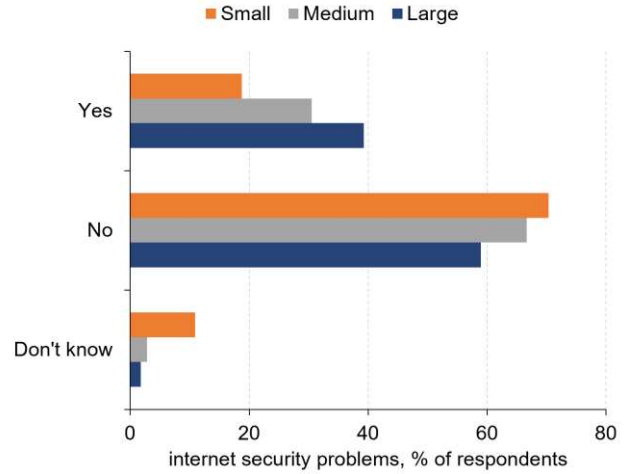
cyber security incidents.[1] Our survey asked businesses whether they experienced any cyber security incidents in 2018. Charts 1 and 2 summarise these survey responses.

Chart 1: Businesses experiencing cyber security incidents in 2018 (proportion (%), by sector)



Source: Ai Group

Chart 2: Businesses experiencing cyber security incidents in 2018 (proportion (%), by business size)



Source: Ai Group

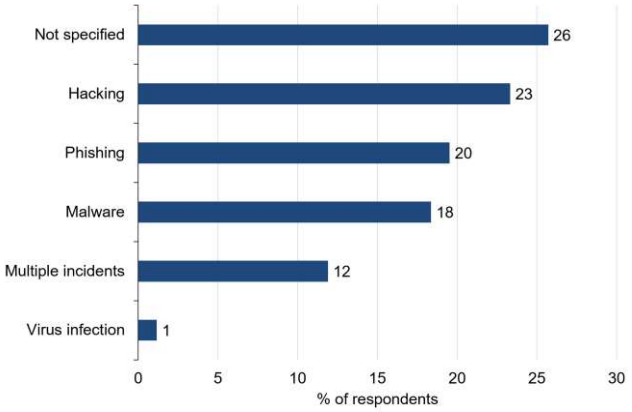
32% of businesses reported that they experienced a cyber security incident of some kind. This was a relatively high number, highlighting that businesses in Australia were susceptible to such incidents and were not isolated from an increasingly connected world. And given that there may be undetected incidents that are unknown and therefore not reported, the numbers could be higher.

Construction businesses reported a higher level of cyber security incidents, although manufacturing and services sectors were not immune either. Similarly, larger businesses reported a higher number of incidents than smaller businesses, though smaller businesses still reported incidents.

[1] Further information about what actions businesses took and invested in with respect to cyber security can be found in our report: https://cdn.aigroup.com.au/Reports/2019/AiGroup_Fourth_Industrial_Revolution_Report.pdf.

The survey respondents that experienced a cyber security incident were also asked to elaborate further about their experience. As can be seen in the Chart 3, the top three most common incidents arose from hacking,[2] phishing and malware. Compounding this, some businesses experienced multiple incidents including virus infections, hacking, malware, phishing, and denial of service.

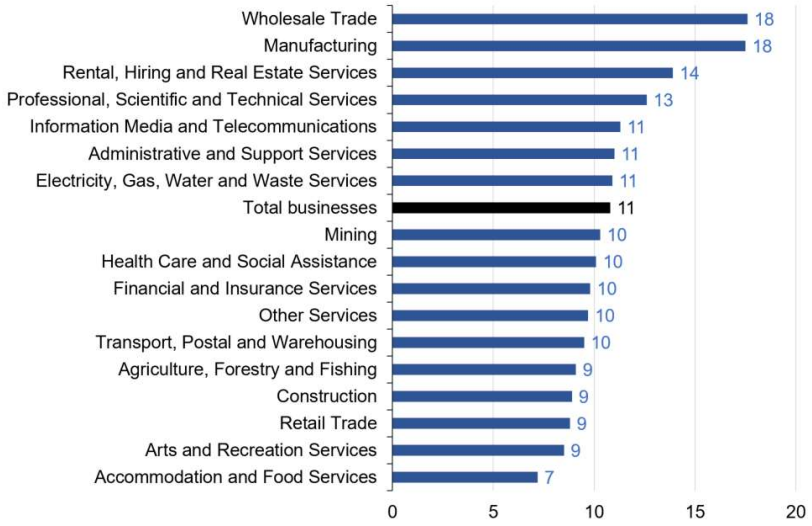
Chart 3: Types of cyber security incidents for businesses in 2018



Source: Ai Group

By way of contrast, the ABS reported that 11% of businesses that it surveyed had experienced a cyber security incident in 2017-18, while 18% did not know.[3] A higher proportion of large businesses reported incidents (19%), followed by medium (17%), small (13%) and micro (9%). Compared to other sectors, wholesale trade and manufacturing reported higher incidents (18%) (see Chart 4).

Chart 4: Businesses experiencing cyber security incidents in 2017-18 (proportion (%), by sector)



Source: ABS

Of the businesses in the ABS survey that experienced a cyber security incident, the impact which

[2] Note: "Hacking" was not defined by the respondents so could possibly fall under other types of cyber security incident categories.
[3] ABS, 8167.0 – Characteristics of Australian Business, 2017-18.

affected most was downtime of service (52%) (see Table 1).[4] This was followed by corruption of hardware or software (38%), loss of staff productivity (33%), and corruption or loss of data (29%). These were common major impacts across different business sizes.[5]

Table 1: Impact of cyber security incidents for businesses in 2017-18 (proportion (%), by business size)

Factor	Employment size				Total
	Micro	Small	Medium	Large	
	0–4 persons	5–19 persons	20–199 persons	200+ persons	
Corruption of hardware or software	35.3	41.1	38.1	23.8	37.7
Corruption or loss of data	27.3	33	21.3	27.7*	28.7
Downtime of service	48.9	54.9	55.9*	54.5*	52
Website defacement	6	5.2	5.6	2.3	5.6
Theft of business, confidential or proprietary information	6	10	6.3	4.1	7.5
Loss of income	14.5	11.1	9.4	8.5	12.5
Loss of staff productivity	26.7	36.3	45.1	50.5*	32.7
Other impacts	1.6	3.7	6.3	6.5	3
None	17.1	15.9	14.3	18.2	16.3

*Note: Factors are shaded depending on prevalence of factor within each employment size subset. 'None' are not included in the shading. * This table includes an estimate that has a relative standard error of 10% to less than 25% and should be used with caution.*
Source: ABS

2.2 Business email compromise

Business email compromise (BEC) is reportedly becoming more common. Under the category of phishing, a number of businesses reported in our survey that their email was hijacked by a fraudulent party, whereby the scammer inserted themselves into correspondence around payments or transactions and fraudulently represented themselves as a legitimate supplier or decision maker within the organisation. Unfortunately, in one case, a small manufacturer reported that they lost a significant amount for a business of their size.

Over the last several years, we have heard anecdotes from other SMEs who have lost even more significant amounts of money through more sophisticated and targeted cyber attacks arising from BECs.

While some types of phishing are random, BEC tends to be more targeted because it requires the fraudulent party to make some effort including researching known decision makers within the organisation either at a high level (a practice labelled as "whaling") or other individuals in the organisation (known as "spear-phishing"). Often, compromised businesses are not necessarily large, which highlights another important fact: cyber criminals target smaller businesses as well as larger ones, and the cost impact of such an incident is relatively significant for smaller businesses.

2.3 Ransomware

Over the last several years, ransomware attacks such as WannaCry and NotPetya have gained mainstream attention. Under the category of malware, ten businesses stated in our survey that

[4] Ibid.
[5] The ABS notes that some of the estimates have a relative standard error of 10% to less than 25% and should be used with caution.

they experienced some form of ransomware attack with some being locked out from their own data. Other types of reported malware included malicious software infecting websites, and virus attachments in emails. While it would seem sensible that businesses do not pay ransom, at least one respondent paid a ransom in bitcoin.

2.4 Spam attacks

While often understood to be unsolicited email received in bulk (e.g. junk email), spam can be used for nefarious purposes such as spreading computer viruses, worms, trojans and other malicious activities such as phishing scams. Responses to our survey about spam attacks may be interrelated with other incidents, although it was unclear as to the nature of the spam and therefore unspecified.

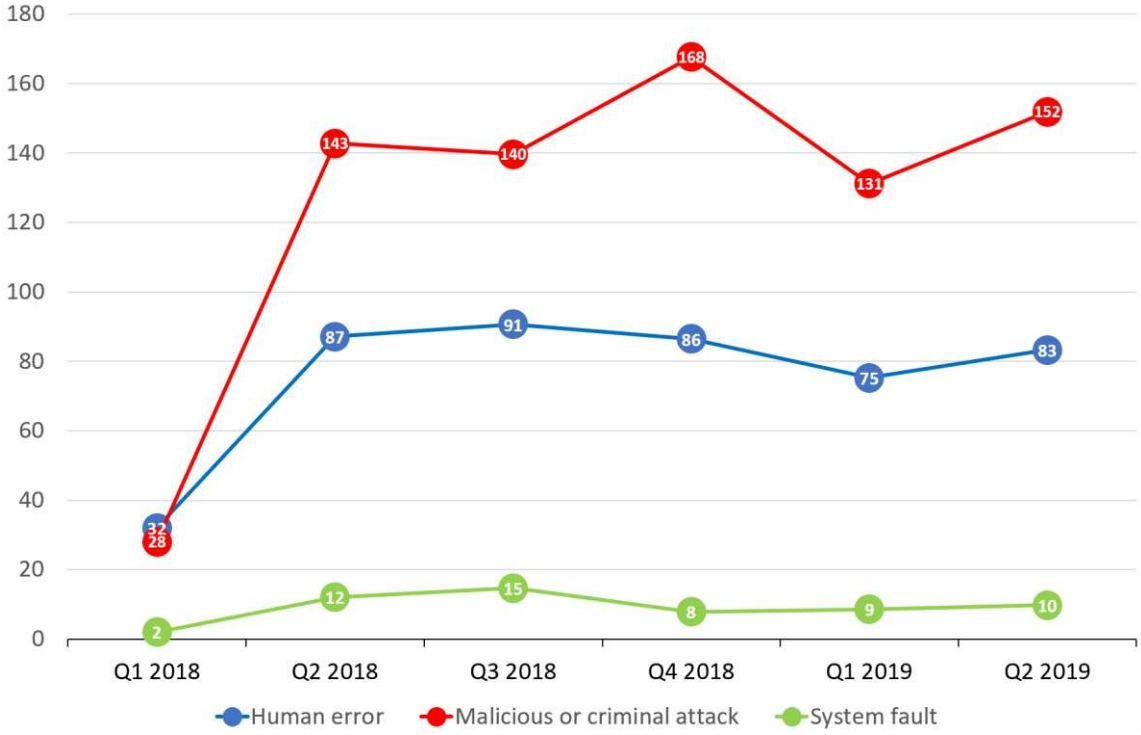
2.5 Hacking and virus infections

A number of businesses indicated that they experienced hacking that targeted their servers or websites. While relatively lower than other types of reported incidents, virus infections do still exist. Businesses need to be mindful of basic cyber security hygiene as well as alert to more advanced forms of attacks.

2.6 Data breaches

Chart 5 below shows the number of data breaches reported to the Office of the Australian Information Commissioner (OAIC) since the NDB Scheme commenced in February 2018.

Chart 5: Notifiable data breaches since NDB Scheme commenced (by breach category)

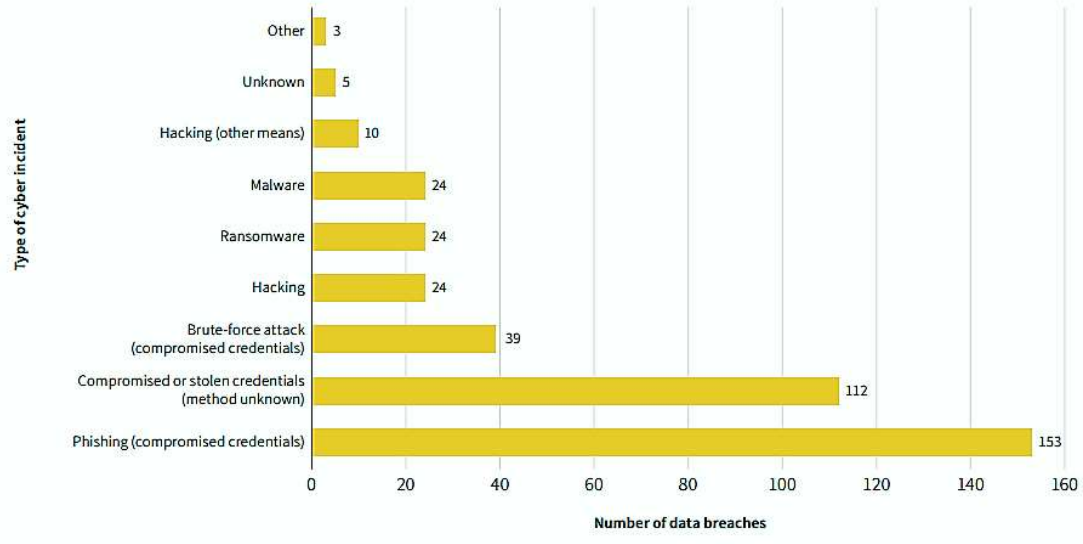


Source: OAIC

By the end of June 2019, there were over 1,270 data breaches reported to the OAIC since the

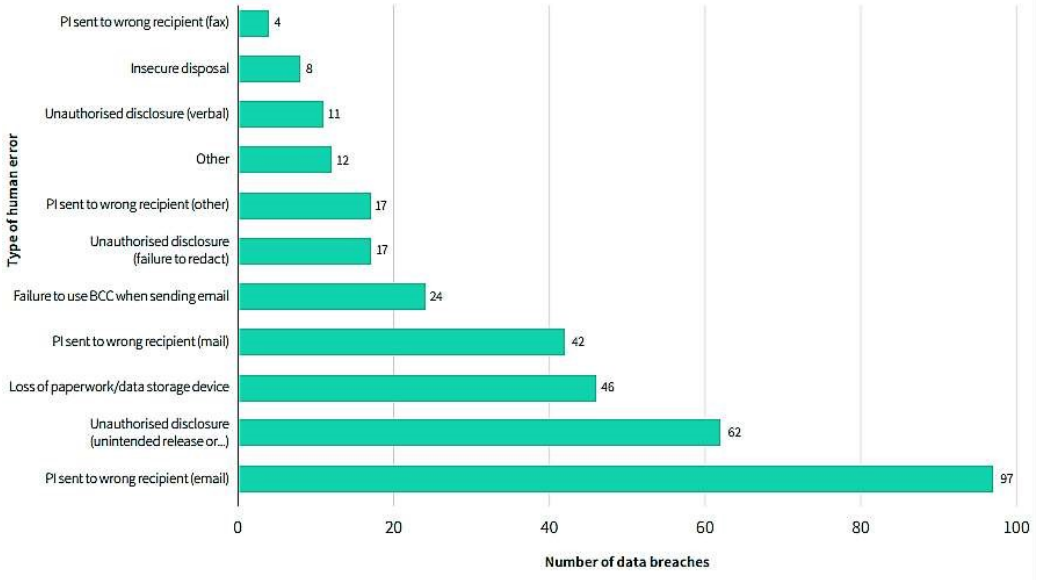
NDB Scheme commenced.[6] Over this period, malicious or criminal attacks greatly contributed to these data breaches (60%), followed by human error (36%). System faults (4%) were rarely a factor.

Chart 6: Notifiable data breaches caused by cyber security incidents, 1 April 2018 – 31 March 2019



Source: OAIC

Chart 7: Notifiable data breaches caused by human error and system faults, 1 April 2018 – 31 March 2019



Source: OAIC

Delving deeper into the data, the OAIC provided a breakdown of the types of cyber security incidents that gave rise to data breaches from the period of 1 April 2018 to 31 March 2019 (see

[6] OAIC, Notifiable Data Breaches Quarterly Statistics Reports (January 2018 – March 2018, 1 April – 30 June 2018, 1 July – 30 September 2018, 1 October – 31 December 2018, 1 January 2019 – 31 March 2019, 1 April 2019 – 30 June 2019).

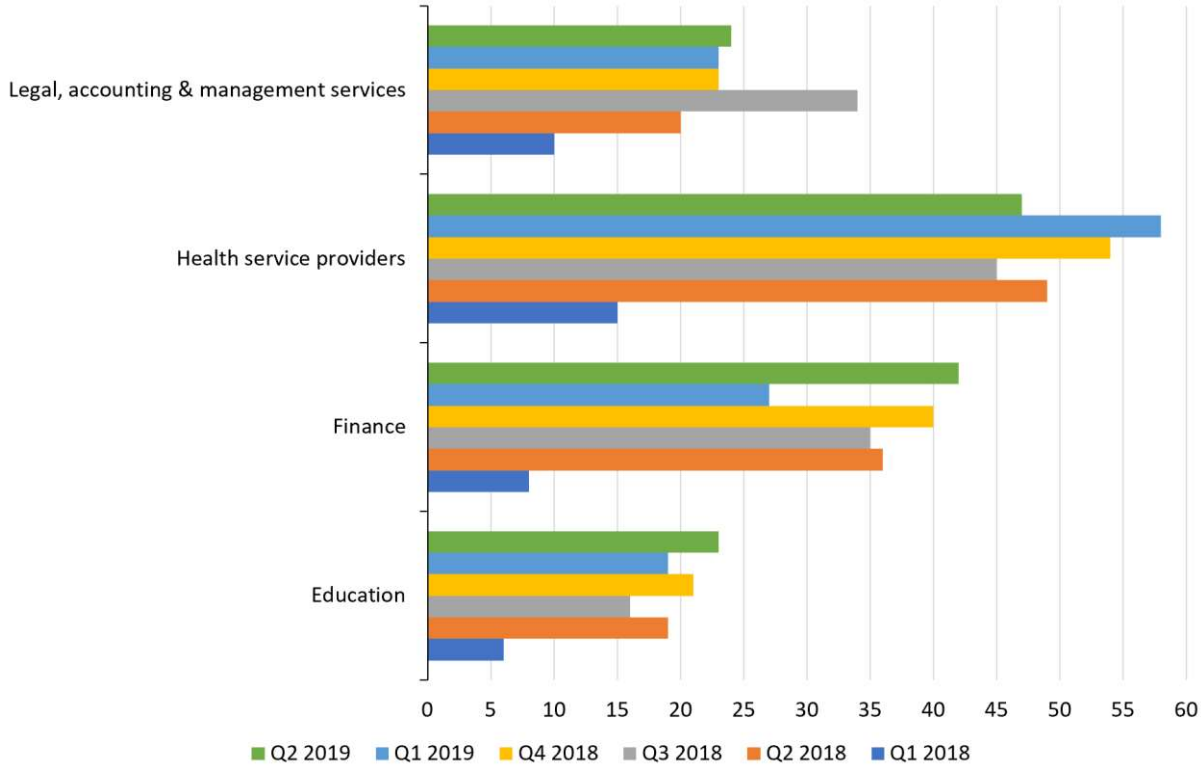
Chart 6).[7] For the same period, the OAIC also categorised the type of human errors and system faults that resulted in data breaches (see Chart 7).[8]

These causes for data breaches point to the need for cyber security hygiene within organisations, as well as more general improvements in internal management of personal data to minimise human errors. And according to a Telstra report, human errors were "often caused by inadequate business processes and employees not understanding their organisation's security policies".[9]

Of the breaches reported to the OAIC since the NDB Scheme commenced, industries that have regularly appeared included: health service providers (21%); finance (15%); professional services (legal, accounting and management) (11%); and education (8%) (see Chart 8).[10] Given how much personal data are handled in these respective industries, this should be no surprise. Of greater concern was that these sectors service other industries so others were not immune.

The fact that there was a steady rate of data breaches being reported from a diverse range of industries highlight the need for additional government support.

Chart 8: Notifiable data breaches since NDB Scheme commenced (proportion (%), by top sectors)



Source: OAIC

[7] OAIC, "Notifiable Data Breaches Scheme 12-month Insights Report" (Report, May 2019), p. 10.
[8] Ibid, p. 12.
[9] Telstra, "Breach expectation: the new mindset for cyber security success" (Article on Telstra website, April 2019).
[10] OAIC, above n 6.

3. Leadership and responsibilities

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

We support the view that cyber security is a shared responsibility across Government, industry and individuals. Akin to safety, it is everyone's responsibility to ensure their workplace provides a safe and secure environment. This means everyone needs to properly understand their role and there should be proper systems in place to provide a secure and resilient environment against cyber security threats.

And our organisations are only as strong as their weakest link. As discussed above, the latest NDB data breach analysis shows that a high proportion of data breaches were due to human error. Therefore it is not only about having cyber security technology to mitigate data breaches.

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

It is positive that more organisations including Government departments and bodies have incorporated cyber security as part of their vernacular. However, we consider that further improvement is required to Government's coordination and engagement with industry and the community on cyber security matters.

We recommend that the following issues require the Government's attention:

- There are currently multiple Government departments and bodies that are involved in cyber security matters in some shape or form – these include (to name a few): Australian Competition and Consumer Commission (ACCC); Australian Communications and Media Authority (ACMA); Australian Cyber Security Centre (ACSC); Attorney-General's Department; Australian Small Business and Family Enterprise Ombudsman (ASBFEO); Australian Signals Directorate (ASD); Australian Security Intelligence Organisation (ASIO); Australian Cyber Security Growth Network (AustCyber); eSafety Commissioner; OAIC; Department of Communications, Cyber Safety and the Arts; Department of Defence; Department of Education; Department of Home Affairs; and Department of Industry, Innovation and Science. With multiple entry points on cyber security matters, this can create inconsistent experiences for industry and the community in engaging with different parts of Government. Consideration needs to be given to the formation of a central and independent coordinating body to provide common approaches across the sectors and levels of Government.

- Different Government departments and bodies engaged in cyber security can also create overlapping responsibilities and potentially conflicting objectives and outcomes. For example, positive public initiatives such as AustCyber promote building a cyber security industry. On the other hand, the controversial TOLA Act developed by the Department of Home Affairs has the potential to weaken existing cyber security and privacy of all Australians.

- There may also be industry and community confusion, limited awareness or recognition of Government's role with respect to cyber security. In our survey, a very small number of businesses indicated that they sought government assistance in 2018 when they

experienced a cyber security incident (6%). Where businesses sought government assistance, these included: access to guides; government website assistance with cyber risk planning; advice on upgrading password strength; advice on regulatory reporting around payroll and superannuation; and subscribing to CERT, Joint Cyber Security Committee and Government Security Advisory Body. Reasons for this low rate of engagement with Government is unclear.

The 2016 Strategy set an overarching framework which included the establishment and allocation of resources for a number of key government responsibilities. These included the Minister Assisting the Prime Minister for Cyber Security, Special Adviser to the Prime Minister on Cyber Security, Ambassador for Cyber Affairs, AustCyber, and ASD. Unfortunately, a Minister dedicated to cyber security with the responsibility to develop expertise on cyber security matters and advocate within the Australian Government for industry no longer exists. We consider this role is critical and would help to resolve the above issues. Therefore, this type of Minister should be reinstated that can take a holistic view, have full responsibility for managing cyber security policy and can operate across relevant departments.

We consider that addressing the above issues will also help to efficiently allocate Government responsibilities to coordinate and respond to cyber security matters.

Question 4: What role should Government play in addressing the most serious threats to institutions and businesses located in Australia?
Question 5: How can Government maintain trust from the Australian community when using its cyber security capabilities?
Question 17: What changes can Government make to create a hostile environment for malicious cyber actors?
Question 20: What funding models should Government explore for any additional protections provided to the community?

Our comments on questions 4, 5, 17 and 20 are closely associated and are considered together in this section.

At a high level, Government has a leadership role to be a trusted confidant and spokesperson for attributing cyber security attacks against institutions, businesses and the community. This could be another function for a Minister with a dedicated focus on cyber security, as discussed above.

Public bodies such as in law enforcement also have a role to support organisations. As mentioned above, we have heard anecdotally from SME businesses about their experiences with BECs. These incidents are becoming more frequent, partly enabled – ironically – by advances in technology, leading to innovative criminal business models like Ransomware-As-A-Service and use of cryptocurrency to enable payment to hackers. It has also been argued that cyber criminals are more responsive than enforcement bodies, who have limited resources to address these threats.

To highlight the scale of the issue, experts have suggested that global cyber crime is now more lucrative than the narcotics trade.[11] Unfortunately, law enforcement resources for tackling cyber security are significantly less than those directed against narcotics. Given the rapidly evolving state of cyber threats and attacks, it is essential that our law enforcement bodies are sufficiently resourced, not only for protecting our national security, but also to protect businesses and the community against global cyber crime.

[11] Cybersecurity Ventures, "2017 Cybercrime Report" (Report, November 2017), p. 3.

While not raised in our survey, we have also received anecdotal feedback from businesses, especially SMEs, about the costs arising from new legislation such as the NDB Scheme. Other data and privacy legislations such as the EU GDPR and CDR (which is being developed for specific sectors), as well as the controversial TOLA Act, also present an additional regulatory burden and challenge for a range of businesses. Government support for businesses to meet these obligations may be required.

And while the TOLA Act requires amendment, businesses in the meantime are struggling to understand its implications for their legal and contractual obligations, regulatory costs and global competitiveness. The Government needs to fund outreach and information resources to address these issues.

Working with, supporting and protecting industry and the community, as described above, will enable Government to build trust while also making it a hostile environment for malicious actors and serious threats.

4. Consumer protection

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

Firstly, industry clearly has commercial interests in ensuring that their business and customers' transactions are protected.

Customer protections are certainly important. When implemented, it should govern the requirements in the design and implementation of security in products and services that meets an appropriate cyber security standard.

It is worth nothing that consumers are currently afforded with protections under the Australian Consumer Law and Privacy Act. Substantiated evidence will be required if there is a view that the current protections are inadequate, supported by proper consultation with relevant stakeholders to properly identify any problems and develop options to address any identified issues.

Question 7: What role can Government and industry play in supporting the cyber security of consumers?
Question 16: How can high-volume, low-sophistication malicious activity targeting Australia be reduced?
Question 22: To what extent do you agree that a lack of cyber awareness drives poor consumer choices and/or market offerings?
Question 23: How can an increased consumer focus on cyber security benefit Australian businesses who create cyber secure products?

A theme common to questions 7, 16, 22 and 23 is the importance of education and raising cyber awareness.

Businesses and individuals need to be better informed about good cyber security hygiene. This is especially important to manage high volume, low sophistication malicious activity. Businesses can also be consumers. Raising cyber awareness through education and training will be key to

helping consumers understand how to protect their data. This is an area where support from Government and industry can play an important role.

In partnership with industry experts, Ai Group runs cyber awareness events for businesses from time to time. Based on the anecdotal feedback, there appears to be a range of reasons for why there may be perceived barriers against proper cyber security investment which can be categorised into several areas: costs; priorities; resources and capability; and awareness and education.

Some businesses have told us that the cost to invest and implement cyber security measures is expensive compared to the risk of an attack. For example, for medium-size to larger businesses, the cost of insurance against ransomware attacks or rebuilding a system containing critical data may be disproportionately more expensive or too difficult compared to the option of paying for a ransom.

For smaller businesses, the resources and capability to manage cyber security are likely to be limited – often little more than the use of basic cyber security technology, allocation of responsibility to an employee with general IT skills or an outsourced IT service provider.

The problem may be further exacerbated by a lack of awareness about good cyber security hygiene. An example was a local defence subcontractor who was infiltrated by a hacker several years ago, which made global news. According to reports, this local company lost a significant number of commercially sensitive documents for defence-related projects including the Joint Strike Fighter program.[12] This incident had three particularly alarming features. Firstly, the company was made more vulnerable by a combination of several poor cyber hygiene practices, including use of very basic default passwords and old unpatched software. Secondly, the breach began in July 2016, was not discovered until November 2016, and only publicly reported in October 2017 (almost one year on). Thirdly, and of most concern, the company in question was a small engineering firm of about 50 employees, with just one IT staff member, which could describe a great many Australian businesses. They may have thought "my business is too small to attract the attention of hackers", which is a common response that we hear from smaller businesses.

Notwithstanding the above, we have seen improvements in business investment in cyber security. Of businesses surveyed by Ai Group, 79% indicated that they invested in cyber security measures in 2018. While our latest survey did not explore other drivers for cyber security investment, the higher proportion of businesses proactively investing in cyber security compared to our previous survey suggested a dramatic shift in business attitudes. This may possibly be due to increasing awareness about cyber management hygiene, and compliance with new privacy and data breach legislations such as the NDB Scheme and EU GDPR.

Separately, the ABS asked businesses about the importance of cyber security technology in 2017-18.[13] The ABS data was less optimistic than Ai Group's findings.[14] A high proportion of businesses (46%) did not see any value at all, closely aligned with micro and small businesses (52% and 42%, respectively), compared to medium (23%) and large (8%) businesses. The accommodation and food services sector valued cyber security the least (no importance at 59%). Conversely, large businesses valued cyber security technology the most (major value at 52%), as well as the financial and insurance services sector (29%).[15]

---

[12] ZDNet article, "Secret F-35, P-8, C-130 data stolen in Australian defence contractor hack" (11 October 2017).
[13] ABS, above n 3.
[14] Ibid. Note: Differences in results between Ai Group and ABS survey data may reflect differences in sampling and data definitions. The ABS sample for *Business Use of IT* includes micro, sole trader and non-employing businesses. Ai Group survey samples exclude these very small and non-employing businesses.
[15] Ibid.

Despite the differences between Ai Group and ABS data, there was still a proportion of businesses that did not invest or value the importance of cyber security technology or other measure. As with safety, cyber security is an ongoing risk management consideration for any business. Lack of business investment suggests that either more work could be done to improve cyber security posture, or that some businesses feel they already have adequate levels of protection.

Ai Group is making continued efforts to improve business awareness about the laws and mitigating data breaches. We would welcome the opportunity to work closely with Government and industry to elevate business awareness with useful information such as from the OAIC.

5. Collaboration and regulation

Question 10: Is the regulatory environment for cyber security appropriate? Why or why not?
Question 11: What specific market incentives or regulatory changes should Government consider?
Question 18: How can governments and private entities better proactively identify and remediate cyber risks on essential private networks?
Question 21: What are the constraints to information sharing between Government and industry on cyber threats and vulnerabilities?

Common themes relevant to questions 10, 11, 18 and 21 are the need for better collaboration to respond to cyber security issues and understanding the role of regulation in this context.

It is critical that there is proper collaboration between government and industry to tackle modern cyber security threats. Collaboration enables sharing of information about threats. It is therefore important that collaboration is encouraged in a safe environment where businesses can share threat information without being punished. This requires a light-handed approach by Government that encourages – rather than penalises – an environment of open collaboration. A collaborative environment can also be conducive to developing innovative solutions to counter cyber security and make us globally competitive.

As one member commented in relation to constraints to information sharing:

> *Understanding constraints and an open discussion on which are critical or negotiable would be of significant assistance in assuring effective delivery of cyber controls. Increased sharing of information, whilst taking into account risk and exposure of that information, will assist in a more effective and consolidated approach to cyber protection.*

With respect to threat identification and management, traditional forms of regulation have been criticised for being inflexible and slow to respond to rapidly evolving threats and pace of technological change. Governments tempted to over-use these regulatory sticks need to consider a different approach if it wishes to achieve proper collaboration to tackle modern cyber security threats.

Regulation can also either make or break the growth of an industry at its early stages of development or going through a period of transition – in this case the Fourth Industrial Revolution. In this context, there are opportunities to build a cyber security industry as well as a *cyber secure* industry. The extent to which businesses are regulated can act as an investment barrier and diminish our attractiveness relative to other jurisdictions.

While regulation has a role in addressing reasonable public concerns such as around security, safety, privacy and environmental issues, there are also often alternative approaches to the regulatory stick. Regulatory barriers should only be introduced where there are clear net community benefits.

Depending on the identified policy issue, regulation may be an option, as well as non-regulatory measures. The issues need to be understood and developed further before an appropriate policy response can be considered.

Unfortunately, we have been alarmed by recent heavy-handed interventions that seek to eliminate some forms of risk rather than manage them, while ignoring the risks and costs to innovation and the economy. Examples of these are discussed further below.

5.1 TOLA Act

The TOLA Act was rushed through Australian Parliament last year without full consideration of the impact that this could create for a broad range of stakeholders. Legitimate concerns about the legislation were raised from a broad range of stakeholders including industry, civil society, and technical and privacy experts. However, the Government response largely ignored the issues raised by passing the TOLA Bill without reflecting stakeholder concerns.

As a consequence, the TOLA risks substantial damage (both real and perceived) to the security, credibility and reputation of Australia's connected systems and products and the businesses and people who use them. Such measures not only add costs to international business, but risk curtailing innovation and limiting the benefits of digitalisation to businesses and their customers. For instance, this has already led to other unintended consequences, including Australia's image overseas in relation to trust in Australian products.[16]This has led to an outcome where businesses are facing a heavier degree of regulatory burden and uncertainty compared to their competitors operating in overseas jurisdictions, with smaller businesses likely to be relatively worse off.

Most importantly, we are concerned that the TOLA Act could lead to the weakening of existing cyber security of businesses and its customers. As mentioned earlier, cyber security threats remain a growing and evolving risk management issue for many businesses. The introduction of the TOLA Act creates an additional layer of risk, which may include impacting on the ability of Government and business to access international security and encryption products, making Australian businesses, Government agencies and the broader community vulnerable to cyber attacks and data breaches.

[16] According to an Australian Strategic Policy Institute Perceptions survey about industry views on the economic implications of the TOLA Act, it found that the third highest ranked concern (71%) was the perception that a company's product might be less secure as a result of the legislation. Not surprisingly, the survey also found that 65% of exporting respondents expected a negative impact on their business activities outside Australia. Concerns remain high for businesses with operations within Australia (57%). This issue goes beyond a global misunderstanding of the workings of the legislation. The damage being done to Australian industry is due to technology buyers and investors around the world having listened to the strong body of international and Australian expert opinion on the risks that the legislation creates for the security of Australian-manufactured technology equipment and systems. For further details, see: Joint submission by Communications Alliance, Ai Group, AIIA, AMTA, DIGI and ITPA to the Parliamentary Joint Committee on Intelligence and Security on "Review of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018" (Submission No. 23, July 2019), Link: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/AmendmentsTOLAAct2018/Submissions; Australian Strategic Policy Institute, "Perceptions survey: Industry views on the economic implications of the Assistance and Access Bill 2018" (December 2018), p. 3.

In this example, industry has a mutual objective with Government to: protect Australians from crimes such as terrorism; enforce the law; and enable the intelligence, interception and enforcement agencies to effectively do so in a rapidly evolving digital environment. Indeed, Ai Group works closely with Government and its agencies on improving Australia's cyber security. Protecting the security of communications and information between businesses and their customers is of fundamental importance. However, proper collaboration requires proper consultation by Government to ensure that the potentially broad impacts of the legislation are tested by exposure to a cross-section of industry and the broader community. Unfortunately, this did not occur in the development of the Act.

Significant lessons should be learnt from the negative industry and public experience with the TOLA Act, and avoid repeating them again.

5.2 NDB Scheme

The NDB Scheme was introduced with an intention to reduce data breaches. While well intentioned, we consider that the Scheme may only promote a compliance culture, as opposed to a proper proactive leadership and risk management culture. There are still questions as to how integrity and privacy measures can be put in place to mitigate data breaches from occurring in the first instance.

In this regard, a policy or regulatory response is only effective if it properly identifies and targets the problem that it is trying to address. Automatically reaching for penalties may not be the most effective solution, and potentially creates a compliance-only mindset. In other forms of regulation such as safety, business and governments have evolved over decades from pure compliance and concerns about over-regulation to a culture of risk management – this was partly driven by customer and supply chain expectations as they became more informed about safety.

Rather than automatically reaching out for new regulatory instruments, further collaboration will be needed between industry and governments to explore workable and practical remedies such as technological solutions.

Bodies such as the ACSC should be commended for working closely with organisations affected by data breaches. However, as the ACSC has noted, this is help after the fact.[17]

Given that a large proportion of data breaches under the NDB Scheme have been triggered by malicious or criminal attacks, or human error, it is important to tackle these causes and prevent breaches from occurring in the first place. For instance, while the OAIC suggested that awareness of the NDB Scheme appeared to be high, there remains a potential gap in awareness about mitigating data breaches, as well as responding to them effectively if they do arise.[18]

As noted earlier, industries that regularly appear in the NDB reporting include health service providers, finance, professional services (legal, accounting and management) and education. This suggests a targeted approach to cyber security awareness raising is worth considering – sometimes referred to as a “public health” approach where those most vulnerable are targeted with appropriate messaging. In this case, a specific awareness campaign could be developed that targeted the industries that most often appear on the NDB reporting.

[17] OAIC, above n 7, p. 19.
[18] Ibid.

6. Products, services and supply chain, and Standards

Question 8: How can Government and industry sensibly increase the security, quality and effectiveness of cyber security and digital offerings?
Question 12: What needs to be done so that cyber security is 'built in' to digital goods and services?
Question 13: How could we approach instilling better trust in ICT supply chains?
Question 25: Would you like to see cyber security features prioritised in products and services?

The issues raised in Questions 8, 12, 13 and 25 could be addressed through promoting relevant existing standards (for example, International Organization for Standardization (ISO)) and best practices, and explaining how they apply to products, services and supply chains.

By establishing appropriately balanced security requirements, industry can provide products and services to meet their customers' security needs on the one hand, while also being able to deliver capabilities that are cost effective. And an increased appreciation of the value of cyber security features in products and services would be advantageous for both businesses and their customers.

Whichever mechanism is used to build in cyber security protections in products and services, it should establish a common set of cyber security requirements across industry. This may require updating of engineering processes and frameworks to include cyber security as part of design, implementation and testing of products and services.

There are various approaches to tackling cyber security as a trust issue, especially in the supply chain. For example, the Charter of Trust initiative brings together several major global companies who have signed up to a range of principles for establishing trust around cyber security with their customers and partners.[19] Consideration could be given as to whether a similar charter could be developed in Australia.

Another way to build trust, especially in the supply chain, is through a chain of custody (CoC) approach, which some companies currently use. If CoC is too difficult to establish, then alternative approaches will need to be explored such as developing a trusted supplier list.

Cyber security certification is another concept that has been considered overseas. For example, the EU Cybersecurity Act came into force in June this year, which "establishes an EU certification framework for ICT digital products, services and processes. The European cybersecurity certification framework enables the creation of tailored and risk-based EU certification schemes".[20] The Commission considers that certification is a way to increase trust by enabling transparency about the security of products and services. On its face, this appears to be an attractive proposition. However, there will be issues that need to be addressed in relation to its implementation, such as being: meaningful to consumers; economically viable for providers of

[19] The Charter of Trust can be accessed here: https://new.siemens.com/global/en/company/topic-areas/cybersecurity.html.
[20] European Commission, "The EU cybersecurity certification framework" (Policy, July 2019), https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework.

products and services; fit-for-purpose; internationally recognised; and harmonised with other approaches. Although a different piece of law, the EU GDPR is an example where it was also recently introduced (last year) and there are currently unresolved issues and challenges with its own implementation: "organisations feel the Regulation has not lived up to its objectives and has presented practical difficulties, despite their dedication to implementing the new requirements".[21] As the EU cyber security certification scheme is relatively new, caution should be taken if Australia were to consider either to adopt this or implement a similar approach – the scope and potential impact of the new scheme on individuals and businesses in Europe and elsewhere is still unclear and untested.

More broadly, standards are fundamental to promoting digitalisation because they can enable an ecosystem for technological innovation, competition, international trade and interoperability. Standards, when called up by regulation, offer a mechanism to quickly respond to changing markets. Australia's regulatory and standards framework needs to be sufficiently flexible to accommodate rapid changes in technologies that lead to new types of business models and competition, while also protecting consumers' interests.

Much global standards work seeks to address broad systems approaches to significant challenges, including cyber security, as well as other related topics such as smart factories, smart grids, smart cities, Internet of Things (IoT) and Industry 4.0. These challenges require a new level of coordination and effort, and development of new ways to exchange knowledge between the public and private sectors, academia, standards and conformity institutions.

It is vital that Australian industry and consumers have support and access to all international fora involved in standards development (particularly ISO and the International Electrotechnical Commission (IEC)) to ensure our national interests are preserved. This will allow for effective contribution to standards development at an ideal stage in which products and services are still under development. Australia is generally known to play a strong role in standards development. Accelerating technological change makes this role even more important to facilitate fast adoption of new technology and realisation of its benefits.

More generally, Australia should strive for a more judicious and effective mix of standards and regulation in lifting public safety, consumer confidence and business performance.

There is considerable potential for the more effective use of consensus-developed standards in addressing a range of economic and social opportunities and challenges. In some cases, standards can work alongside formal regulatory approaches (such as when standards are called up in regulatory instruments) and at other times as a lower-cost substitute for formal regulation.

There has been a tendency for government to move away from the use of Australian standards. While international consistency and efficiency have clear value, international standards development processes may be unduly influenced by particular interests without adequate opportunities for Australian input reflecting domestic expertise, local conditions and needs. The Australian Government should continue to help fund Australian involvement in international standards development and it should ensure that an Australian filter is applied before the adoption of international standards in Australia.

There is also a disturbing tendency for Australian government agencies to forego the well-regarded model of the transparent, consensus approach to the development of standards in favour of rules and regulations developed by the agencies themselves, including with respect to product energy efficiency. Government agencies typically do not have the technical expertise, the practical experience or the proficiency in effective and structured consultation with industry and others in the community. The result is often sub-standard, and Government should be more willing

[21] Centre for Information Policy Leadership, "GDPR One Year In: Practitioners Take Stock of the Benefits and Challenges" (May 2019).

to back and expedite the use of the more transparent consensus driven standards development model.

7. Professional development and growth

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

AustCyber's 2018 update to its Cyber Security Sector Competitiveness Plan reported that there was a real and severe shortage of cyber security skills shortage in the Australian workforce:

> *… the sector may be short of 2,300 workers today, costing more than $400 million in lost revenues and wages. With strong demand forecasts, the pressure is unlikely to ease soon. The latest assessment indicates Australia may need up to 17,600 additional cyber security workers by 2026 to fill this gap and enable the sector to meet its potential.*[22]

Positive initiatives such as AustCyber promote the development of a cyber security industry in Australia. Support for this body should therefore continue. Developing this industry will lead to creation of jobs and demand for access to high quality cyber security professionals.

To respond to the current skills shortage and anticipated growing demand, developing a market of cyber security professionals in Australia requires a multipronged approach including access to talent in the immediate term and developing talent in the medium to long term. This means:

- Giving stronger priority to the skilled migration stream within the permanent migration program and especially to the demand-driven components of skilled migration including for cyber security.
- Developing the current workforce which not only develops basic cyber awareness skills that are fundamental to the modern worker, but also developing more advanced knowledge as a pathway to becoming a cyber security professional.
- Developing the future workforce in all education and training sectors from primary level up through to tertiary level.

While there have been positive responses from the education system including at the tertiary and VET levels, challenges remain to close the skills shortage gap according to the AustCyber report.

It therefore recommends the following to address cyber security skills shortage in the long term:

> *Many universities and TAFEs are struggling to compete with the private sector to attract and retain teaching staff. Education providers need to keep attracting demand from the best and brightest students. High schools could help increase awareness of this career path by incorporating cyber security more strongly as a subject in their curricula. New cyber security courses should be industry-focused and include opportunities for work-integrated learning, such as apprenticeships, to truly prepare students for jobs.*[23]

[22] AustCyber, Cyber Security Sector – Competitiveness Plan: 2018 Update, p. 14.
[23] Ibid.

This leaves a potential skills shortage gap in the medium term:

> *… the sector needs to offer more transition pathways for workers to move from the general IT sector and other industries into cyber security roles. There are more than 250,000 workers in the IT sector who could easily move into similar roles in cyber security. However, the transition is too reliant on large employers. Opening up pathways for workers to independently transition, through better information about cyber careers and access to more low-cost training places, can improve that flow.*[24]

We strongly support AustCyber's suggestions. The report also goes into further depth about various aspects of the cyber security skills shortage challenge, amongst other things, which we encourage Government to explore further.

There is also an opportunity for Government to take leadership in developing a market for cyber security professionals by building capability within Government to tackle cyber threats. This will likely require employing skilled professionals. In the medium to long term, this could create another pathway for cyber security professionals to work in the private sector.

For businesses involved in cyber security projects, focused training and development, along with the development of cyber capabilities within these projects, is one of the best ways to build capability inhouse. This could be boosted by engaging with foreign experts to provide guidance, however this may be subject to security restrictions depending on the project.

8. Critical infrastructure or systems

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

Each business will have its own risk profile, with some only requiring good cyber hygiene. Others such as critical infrastructure or systems will require a much higher level of security and resilience. An example of a particular industry network that should be treated as critical is Defence. The earlier example about an SME local defence subcontractor who was infiltrated by a hacker demonstrates a need to identify networks that interface with Defence which should be classified as critical and requires stronger cyber defences.

[24] Ibid.