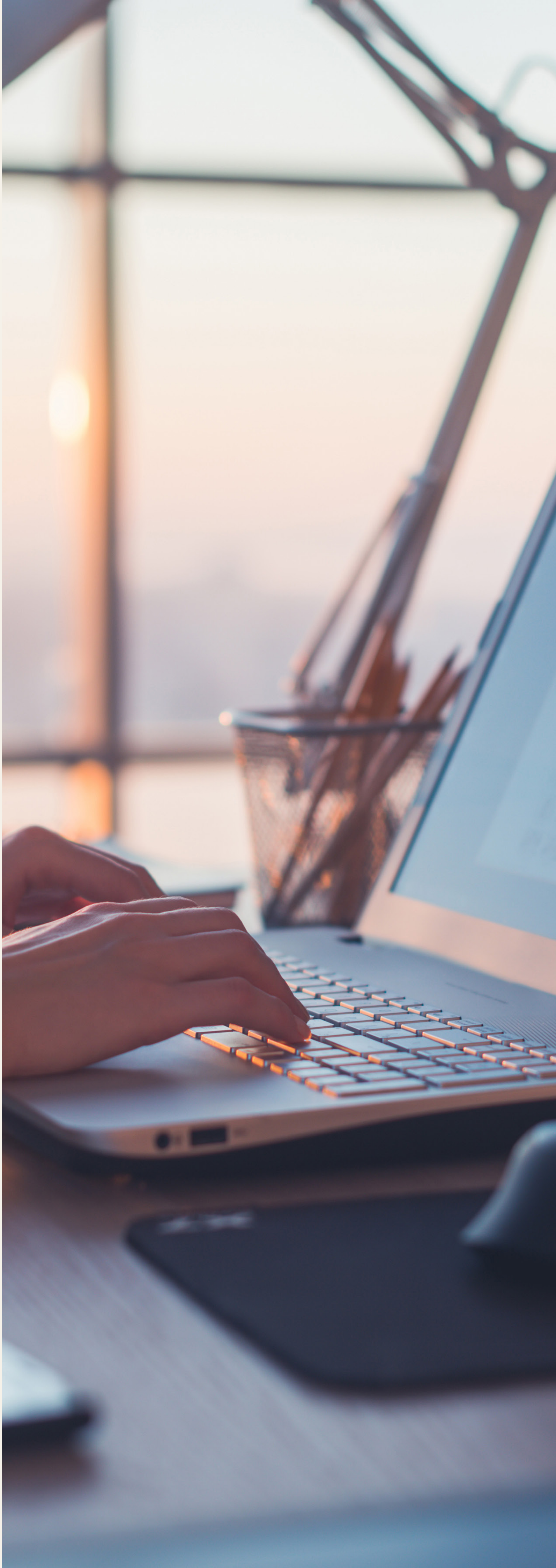
Australia's 2020 Cyber Security Strategy

Commonwealth Bank's submission to the Government's Call for Views

November 2019

CommonwealthBank

Contents



Foreword

At CommBank we take cyber security very seriously. Cyber security is an essential enabler of the applications and digital technologies we provide our customers to bank with confidence online. However, cyber security is not just about keeping the bank's and our customers' data safe and secure. We believe we can and should play a broader role in securing Australia's digital ecosystem. That's why CommBank staff are involved in initiatives to help build cyber security skills at schools and universities, speaking face-to-face with business and personal banking customers about their security, and making great cyber security resources including eLearning available to anyone, whether or not they are a CommBank customer.

We are very pleased to contribute to the Government's 2020 Cyber Security Strategy. As a nation, we have an opportunity to build on some of the successes of the 2016 strategy, such as:

- The co-location of the Government's cyber security functions in the Australian Cyber Security Centre (ACSC) and the establishment of the Joint Cyber Security Centres (JCSCs);
- Provision of support and technical assistance by the ACSC and JCSCs in major cyber incidents;
- Publication of cyber security guidance for both large enterprises and small businesses; and
- Support of programs and competitions to encourage student interest in cyber security.

The next phase of our national cyber security journey must be equally ambitious. Australia is a prosperous and technologically advanced nation, which makes us an attractive target for cyber criminals. We need to make Australia a hard environment for cyber criminals and increase public awareness of cyber crime. Government and industry must align efforts to help build cyber aware businesses and individuals – at all stages of life – and create a national cyber security culture.

Our economic future is, to a large extent, digital. We need to pursue a vision of Australia as a net exporter of cyber talent and innovative technology. This will require an education system that produces cyber experts of the future, capable of keeping our businesses and institutions secure as they embrace the next phase of digital innovation. We also need to create conditions in which cyber and technology industries can flourish.

We need to give Australian businesses every advantage we can in fighting cyber adversaries, recognising that, in a connected economy, an incident affecting one organisation will often have a significant ripple effect across its supply and customer chains. This will require improved sharing of cyber threat intelligence and greater cooperation between industry and government.

We hope this submission is one of many valuable contributions to a public discussion that will inform a far-sighted and robust national strategy for securing our digital future.

Pete Steel
Chief Information Security Officer
CommBank

Executive summary

Our view of the Australian threat environment

The Australian threat environment is subject to many of the trends affecting comparable economies. These include increasingly sophisticated adversaries targeting weak links in supply chains, and using native applications on targeted systems to make it harder for an organisation to detect their attack. Attackers continue to target humans with social engineering attacks. Phishing and fraudulent email scams are enduring features of the threat landscape – but attackers are constantly refining their tactics and techniques and exploiting emerging technologies to make these attacks more credible.

Our threat environment also has some unique features. Attackers use Australia as a 'testing ground' for new forms of malicious software. Australia suffers a cyber skills shortage that, in particular, hampers the capabilities of small- and medium-sized businesses to prevent, detect, and respond to cyber attacks. In addition, our concentrated market for IT suppliers and service providers may provide a leveraged return on adversaries' investment in attack tools.

The role of Government in addressing the most serious threats to institutions and businesses located in Australia

In our connected economy, an attack on one organisation can have impacts across customers and supply chains. Accordingly, we believe the Australian Cyber Security Centre (ACSC) should receive additional resources to help organisations facing major cyber incidents, subject to clear frameworks for both engagement and prioritisation of response and recovery activities. The ACSC should play a central role in providing cyber threat intelligence to industry partners: providing analysis of the incidents with which it is involved; promptly declassifying government intelligence that can help businesses to remain secure; and acting as a central hub for the collection and dissemination of threat intelligence sourced from industry partners.

Addressing the cyber skills gap

Australia needs concerted action across Government, industry and the education sector to become a net exporter of cyber talent and innovation. It is widely acknowledged that Australia faces a cyber skills shortage, but to address this we need rigorous analysis of our economy's cyber requirements and how they can be met.

Cyber safety is a foundational life skill that must be taught in primary schools. High school curriculums must encourage participation – especially by female students - in STEM subjects (Science, Technology, Engineering and Mathematics) that are the foundation of cyber skills. Universities should collaborate, and work with industry, to offer comprehensive, work-relevant cyber security courses that produce graduates capable of meeting the cyber challenges of tomorrow. We encourage continued Government support of cyber challenges and programs that help build technical cyber skills.

Building cyber awareness

It is critical that Government and industry align and coordinate their efforts to make life harder for cyber criminals by raising public awareness of cyber risks. Different groups in society (e.g. older Australians, young people, parents and children) face different risks, have different concerns, and preferred channels for communications. We need a cultural shift towards cyber security that addresses these diverse needs, ideally under an overarching call to action to secure the digital wellbeing of all Australians. There are lessons we can learn from previous successful Australian public information campaigns that have empowered individuals with practical advice, and have tackled hard subjects without sowing fear, uncertainty and doubt.

Government and industry partners also have a role to play in building cyber aware small- and medium-sized businesses. This works best when Government's trusted voice is combined with industry expertise to produce practical, easy-to-follow advice that takes into account the limited time and material resources of many small- and medium-sized businesses.

Ensuring our legal and regulatory framework supports cyber security

Australia's laws and regulations must drive improvements in cyber security standards, but should not stifle innovation. We need to improve supply chain security through legal frameworks that encourage the prompt identification and remediation of security flaws in widely used software and hardware. The Government should actively engage the technology community when it develops legislation and regulations that could impact the competitiveness of our technology industries, or have other adverse effects on our innovation ecosystem. We need to ensure our regulatory and legal framework achieves the desired outcomes of raising cyber security standards and protecting individuals affected by data breaches, but avoids requiring businesses to provide duplicative reporting to different government and regulatory agencies.

Our view of the Australian cyber threat environment

The Government's 2020 Strategy for Cyber Security should aim to create a future in which Australia is a tough and unwelcoming environment for cyber criminals. Cyber crime, in particular, places a significant burden on the Australian economy. However, we cannot measure the cost of cyber crime by its financial impact alone: the loss of trust in the digital economy and the emotional and psychological impact must also be counted. By hardening our environment, we can reduce the diversion of money away from Australia's legitimate economy, and strengthen consumer and business trust in our digital ecosystem. We can achieve this by Government and industry working together to increase public awareness of, and create technical barriers to cyber crime. In addition, Government and industry must collaborate to help meet the challenge of a constantly evolving threat environment through the timely and secure exchange of actionable cyber threat intelligence.

Global threats and trends

CommBank has observed that the Australian threat environment largely mirrors the global threat environment but also has some unique characteristics. Our Cyber Security Centre assesses that Australia faces the following threat trends that are shared with many comparable countries:

- Threat actors are becoming increasingly adept at identifying and exploiting weak points in the defences of organisations – creating an asymmetry where even organisations with robust controls cannot afford to be complacent.
- Threat actors are seeking to exploit supply chains, looking for weak links or opportunities to leverage their efforts by targeting widely used suppliers.
- Cyber attacks continue to target humans as well as machines, with employees and customers of financial services organisations continuing to fall victim to phishing, smishing (i.e. SMS phishing), and automated voice campaigns, despite increased awareness of cyber threats. These attack types are being used for both financial gain (by cyber criminals) and for gaining deeper network access (by sophisticated attackers).
- Sophisticated attackers are increasingly using native tools on targeted systems to avoid detection and reduce their costs (a practice known as "living off the land"). Meanwhile, less sophisticated attackers are gaining access to advanced attack tools. This is making it more difficult for cyber threat intelligence teams to attribute attacks to a particular group or determine the attacker's motive or skill-set, based on modus operandi.

The Australian threat environment

Australia is a wealthy and tech-savvy nation, which has quickly adopted online services for banking, shopping and interacting with Government. 91% of all Australian households are now connected to the internet and 80% of Australians are using the internet for banking[3]. It is no surprise then, that Australians are frequently targeted by financially motivated cyber criminals. Independent research indicates that the customers of Australian financial service providers are tied in second place behind the USA when it comes to the variety of malware that targets them[4].

Several factors provide the Australian threat environment with unique characteristics:

- CommBank's Cyber Security Centre has observed that Australia is used by some cyber criminals as a 'testing ground' for malware, with modifications to existing malware strains debuting in the Australian market before being seen in other jurisdictions.
- The shortage of cyber skills in Australia means that many small- and medium-sized businesses have difficulties in recruiting and retaining the cyber security professionals they require to protect against, detect, and respond to, cyber attacks. (For further details, please see "Addressing the cyber skills gap" below).
- The highly concentrated IT supplier and service provider market in Australia enables sophisticated attackers to gain access to multiple organisations' data and systems by compromising IT service provider 'hubs'. This leverage provides attackers with an enhanced return on their investment in attack tools.

"91% of all Australian households are now connected to the internet and 80% of Australians are using the internet for banking[3]."

Businesses and cyber crime

62%

of Australian data breaches reported to the Office of the Australian Information Commissioner (OAIC) were a result of malicious or criminal attack.

Source: OIAC Notifiable Data Breaches Statistics Report: 1 April to 30 June 2019[1]

94%

of businesses experienced phishing attacks in 2018

Source: Mimecast, Mimecast State of Email Security Report 2019[2]

Enduring threats take on new forms

Cyber threats are evolving into new forms as threat actors increase their capabilities and evolve their tactics, techniques and procedures.

Ransomware

Cyber criminals are finding increasingly sophisticated ways to deploy ransomware, moving well beyond simple phishing campaigns. Recent sophisticated attacks have combined ransomware with other attack tools, enabling lateral movement within the targeted network, increasing administration privileges, and delivering the ransomware payload onto targeted machines.

Business email fraud

Business email compromise (BEC) and executive impersonation scams continue to be a major concern for our business customers. In May 2019, the Australian Competition & Consumer Commission (ACCC) released its 'Targeting Scams' report, which noted that BEC scams were the most financially harmful scam affecting Australian businesses[5]. BEC scams involve an attacker gaining access to the email account of a key person in a business who deals with the transfer and receipt of money. Executive impersonation fraud involves the attacker using spoofed emails and messages that impersonate senior executives to elicit funds from victim organisations. Cyber criminals are making these attacks increasingly sophisticated and plausible through new techniques, such as supplementing fraudulent emails with SMS messages[6], or following-up an email with a call from someone posing as a lawyer[7]. Most recently, we have seen cyber criminals exploiting voice technology to pose as a CEO and convince another senior executive to transfer a large sum to the criminals' account[8].

Emerging threats

CommBank has observed the following emerging threats that will become increasingly prominent in 2020 and beyond:

- We have observed a shift by international and domestic attackers away from economic models that rely on the identification of a few vulnerable victims amongst a very large target set[9]. Attackers are increasingly willing to invest more in targeting specific, high-value targets, such as individuals nearing retirement age[10].
- Cyber criminals are utilising social media and other technology to identify individuals who are more likely to fall victim to major scams (e.g. to identify retirees with access to superannuation), or to identify CEOs and CFOs for business email compromise scams (see "Enduring threats take on new forms" text box to the left).
- Criminals are taking social engineering scams to new heights of plausibility by using fake audio to impersonate senior executives (see text box to the left). We anticipate attackers will continue to develop attacks using so-called 'deep-fake' technology and it probably will not be long until we see scams involving manufactured video too.
- While organisations continue to orchestrate and automate their response activities, attackers are similarly automating and accelerating their attack methodologies. This will open a new front – the battle for speed supremacy – in the fight between organisations and highly skilled threat actors.

Recommendations for Government

- The Government should focus on reducing cyber crime to help prevent the diversion of funds into the illegitimate economy and to maintain public trust in the Australian digital ecosystem. This will require close cooperation between government and industry to increase public awareness of cyber crime and create technical barriers to make life harder for cyber criminals.
- The rapidly changing Australian threat environment and the increasing interconnectedness of supply chains in our digital economy make it imperative that Government and industry improve their cooperation in sharing cyber threat intelligence in a timely and efficient manner.

> **"We have observed a shift by international and domestic attackers away from economic models that rely on the identification of a few vulnerable victims amongst a very large target set[7]."**

The cost of cyber crime

>AUD $60 million

lost by Australian business in 2018 from business email compromise scams

Source: Targeting scams: report of the ACCC on scam activity 2018[11]

USD $6.8m

Average cost of cyber crime to Australian businesses in 2018

Source: Ninth Annual Cost of Cyber Crime study by Accenture and the Ponemon Institute[12]

USD $12.5 billion

Global cost of business email compromise (October 2013 to May 2018)

Source: Federal Bureau of Investigation (IC3) Public Service Announcement July 2018[13]

The role of Government in addressing the most serious threats to institutions and businesses located in Australia

At CommBank, we believe an empowered and well-resourced Australian Cyber Security Centre (ACSC) has a unique opportunity to play a central role in helping institutions and businesses to both prevent and respond to cyber attacks.

We would like the ACSC to increase its capacity to help organisations deal with major cyber attacks. This will require the development of a clear framework for engagement with the ACSC, recognising that, in a connected economy, a major attack against one organisation can have impacts within and across sectors.

The ACSC is also in a unique position to share intelligence with industry through its assessment of the incidents with which it is involved, and by efficiently declassifying and disseminating intelligence to industry partners. However, we believe the ACSC could play an even bigger role: acting as a central repository for industry-sourced threat intelligence, and as a hub for its timely and secure distribution.

Helping organisations respond to significant cyber security incidents

CommBank regards the establishment of the ACSC within the Australian Signals Directorate as a single point of cyber expertise for the Australian Government, together with the formation of the Joint Cyber Security Centres (JCSC), to be amongst the key successes of the 2016 Cyber Security Strategy.

Since its foundation, the ACSC has provided significant support and assistance to Australian organisations that have suffered cyber security incidents. The ACSC has both helped coordinate the response to the incident, and provided deep technical expertise to limit the impact to the organisation and the broader digital ecosystem. The importance of this role will only grow as our economy becomes increasingly connected. The JCSCs have provided a very effective centralised forum for sharing information with other organisations affected by security incidents. This has proved particularly valuable where the compromised organisation is an important element in the supply chain or operations of a large number of other organisations.

Framework for engagement in a major cyber incident

The role of the ACSC and the JCSCs in helping organisations to respond to cyber incidents impacting the country's digital ecosystem could be strengthened by the establishment of a clear engagement framework. This would provide guidance to organisations on when to engage the ACSC, the assistance the ACSC can offer, and the consequences for not engaging. The framework should consider the powers of the ACSC, and options such as mandatory "step-in" powers in specified circumstances.

“Since its foundation, the ACSC has provided significant support and assistance to Australian organisations that have suffered cyber security incidents.”

Prioritisation principles in a major incident

Australia lacks clear protocols or prioritisation mechanisms to facilitate an effective response to a major cyber security incident. The need for such principles is most acute where the compromised organisation provides services to, or holds data on behalf of, a significant number of customer organisations. Recent examples of such attacks demonstrated that the capability of the compromised organisation to analyse and contain the attack could be impaired by the competing demands of its customer organisations to provide the information they need to meet their own regulatory and industry requirements.

The ACSC and industry should work together to develop a model for responding to a major cyber incident that strikes an appropriate balance between containing and minimising the impact of the attack with meeting customer and regulatory demands. This model may be similar in concept to the aviation safety principle of "Aviate, Navigate, Communicate" used to prioritise activities in a crisis[14].

Preparing for the worst

Government should work with major industries and critical national infrastructure providers to develop and maintain the capability to respond to, and recover from, a major cyber attack, which targets one or more industries simultaneously. This will require the development of response plans and scenario playbooks, which must be tested in regular industry-wide, cross-sector exercises to facilitate national response and recovery.

The case for sharing intelligence

The constant evolution of attackers' tactics, techniques and procedures means that a comprehensive and regularly revised understanding of the threat landscape is critical for an organisation to maintain its cyber resilience. The sharing of attack intelligence can enable other organisations to quickly 'immunise' themselves against the same tools and techniques. This dramatically increases the cost to the attacker, as it will need to develop new tools every time they are detected. These factors create a strong case for the sharing of threat intelligence data between cyber security teams working in both the Australian public and private sectors. After all, no single organisation has a complete view of cyber security threats.

We need to create an environment that not only supports high standards of cyber security, but also encourages an organisation to share intelligence on compromises or 'near-misses' it has suffered, without undue fear of criticism and scrutiny. This would remove barriers to effective intelligence sharing and align to the global shift in understanding that even a well defended organisation can suffer a cyber attack, and should be measured against how quickly and transparently it responds.

Exchange of intelligence between industry and government

Intelligence from incidents with which the ACSC assists

The ACSC has a unique and privileged view of the Australian cyber threat landscape by virtue of its role in responding to some of the most significant cyber incidents affecting Australian organisations. Cyber threat intelligence teams in Australian enterprises are relatively well served with threat intelligence that is global or region-specific (e.g. US, or Europe-focussed), but would greatly value more intelligence that focuses sharply on Australia. We would welcome increased resourcing of the ACSC to enable it to produce and disseminate actionable threat intelligence based on its assessment and analysis of the major incidents with which it is involved. In this context, we recommend the ACSC considers resuming publication of the annual ACSC Threat Report (or a more frequently published regular trend report), as this reporting filled a gap in coverage with its focus on the Australian threat environment.

Declassified intelligence

There is also appetite from Australian cyber threat intelligence teams for more declassified intelligence that is timely, actionable and relevant to their organisations.

This would include directly actionable tactical intelligence, as well as more strategic intelligence that provides geopolitical or other strategic context to the developing threat landscape. We acknowledge the administrative and security hurdles to declassifying intelligence and the need for industry to articulate clearly its intelligence requirements to government to better enable this process. However, we also note initiatives such as the UK National Cyber Security Centre's (NCSC) "IOC Machine", which has reportedly accelerated the speed at which sensitive material is declassified into the public domain through automation. This has enabled the NCSC to share more than 1,000 vital indicators of compromise (IOCs) with industry partners each month, which can provide a broad understanding of how an adversary attacks, but can also cover very specific details, such as signatures of malware used or IP addresses associated with an adversary[15].

ACSC as a hub for intelligence exchange across industry

We note the success of the sector-based US Information Sharing and Analysis Centers[16] in coordinating information flow across private sector organisations and governments. We believe Australian organisations would benefit from the ACSC playing an active role as a central repository for the collection and dissemination of cyber threat intelligence sourced from trusted industry partners.

To facilitate greater sharing of intelligence between industry and Government, the establishment of secure channels for exchange of information is an important foundational step to facilitating the ACSC as a hub for public and private sector cooperation on cyber security.

Helping organisations adopt global better practice

The ASX 100 Cyber Health Check report, published in April 2017, collated the results of the voluntary cyber security surveys sent to Australia's top 100 listed companies. This report provided a baseline against which peer organisations could compare themselves and will have spurred some organisations to take steps to improve their cyber security posture.

We believe there is demand from Australian businesses for a trusted reference point for how leading organisations are defending themselves and 'what good looks like' from a cyber security perspective. Accordingly, we recommend Government undertakes a regular survey (e.g. every two years) of leading companies' cyber posture, governance and capabilities, the results of which are reported with analysis and comment from the ACSC on global better practice. We believe this initiative would help secure the Australian ecosystem by enabling organisations of all sizes to more quickly adopt successful cyber security practices.

> **"Australia lacks clear protocols or prioritisation mechanisms to facilitate an effective response to a major cyber security incident".**

Providing focal points for the cyber security community

The JCSCs provide dedicated meeting places for the cyber security community, which are becoming focal points for inter-organisational cooperation. This has proved particularly effective where JCSCs are co-located with the Cyber Security Innovation Nodes. The examples below demonstrate the breadth of opportunity that exists for these spaces to be leveraged – from industry capability building, incident response to awareness and training:

- Launch of the Cyber Security Schools Challenges in New South Wales at the Sydney JCSC (for further details of this initiative to build cyber skills, see the "Addressing the Cyber Skills Gap" section);
- Cross-industry and government cyber security information and intelligence exchanges;
- Information session for members of the Victorian Small Business Mentoring Service on current threats and cyber hygiene presented by representatives of CommBank, the Australian Federal Police, and consultancy ITSafe; and
- Awareness training for executive assistants on the phishing threat, provided by members of the ACSC.

Recommendations to Government

- Government should work with industry partners to develop a clear framework that provides guidance to organisations on when to engage the ACSC in a cyber security incident, the assistance the ACSC can offer, and the consequences for not engaging.
- The ACSC should work with industry partners and across government, including regulators, to develop a model for responding to a major cyber incident that prioritises understanding and containing the attack.
- Government should work with major industries and critical national infrastructure providers to develop and exercise response plans and scenario playbooks for responding and recovering from a major cyber attack that targets one or more industries simultaneously.
- The ACSC should be resourced to enable it to produce and disseminate timely and actionable threat intelligence based on its assessment and analysis of the major incidents with which it is involved.
- ACSC should consider resuming publication of the annual ACSC Threat Report (or a more frequently published regular trend report), as this reporting filled a gap in coverage with its focus on the Australian threat environment.
- Government should seek ways to accelerate the declassification of cyber threat intelligence and its distribution to industry partners, noting the success of the UK National Cyber Security Centre's 'IOC Machine' initiative to automate some of this process.
- Government should consider resourcing the ACSC to act as a central hub for the collection and dissemination of cyber threat intelligence from trusted industry partners.
- Government should establish a secure channel for the exchange of cyber security information and intelligence between government and industry.
- We recommend Government conducts a regular survey (e.g. every two years) of leading companies' cyber posture, governance and capabilities, the results of which are reported with analysis and comment from the ACSC on global better practice.
- Government should continue to fund and support the JCSCs to provide focal points for the cyber security community, hosting information exchanges and events that help organisations and individuals across the Australian economy to be more secure.

Addressing the cyber skills gap

CommBank can envision a future in which Australia is not only able to address the cyber talent shortage it faces, but becomes a net exporter of cyber talent and innovation.

This will require a refreshed approach to cyber security education. We need to start early: cyber safety is a foundational skill and must be integrated into primary school education. High school curriculums must provide both male and female students with the skills and capabilities they need to fully participate in the digital economy. Australia will need to develop a strong network of universities that each offer a world-class, comprehensive cyber security education, and partner closely with industry to produce graduates who are ready to tackle our future cyber security challenges.

If we are to meet the cyber challenges of tomorrow, we will need innovative and scalable cyber technologies. We believe this technology could and should be created here in Australia, taking advantage of our trusted geopolitical relationships, our solid educational foundations, and our national spirit of inventiveness. This would also reap a significant innovation yield for Australia's economy.

Defining the cyber skills shortage

There is no shortage of statistics demonstrating that Australia faces a shortfall in cyber security skills. For example, in 2018, AustCyber reported, "Australia may need almost 18,000 additional cyber security workers by 2026 for the sector to harnesses its full growth potential"[17]. To help address the cyber skills gap, there are a number of excellent existing initiatives, including partnerships between the public and private sectors (detail of some of these follow below). Many of these initiatives focus on building strong technology-based skills for tomorrow's Australian cyber security workforce. This is without doubt highly desirable. However, if we reflect on the cyber skills requirements in CommBank itself, it becomes apparent that our requirements for cyber skills are very broad.

We need people to work across our cyber security team who have quite different professional backgrounds, and may not have come from a 'hands-on' technology background. For example, we need:

- Project managers to effectively implement security controls in an evolving threat and technology landscape;
- Privacy experts to ensure we meet the increasingly complex privacy needs of our customers;
- Organisational change managers to help colleagues understand, and maximise the benefit of, changes to technology and processes that make CommBank and its customers more secure; and
- Legal, regulatory and compliance experts to help us understand and meet our domestic and international regulatory obligations in connection with cyber security.

Given the complexity of the cyber skills shortage, which spans professional disciplines and career stages, we can see a role for government in conducting deeper research into the detailed requirements for cyber skills in the current and future Australian workforce. A detailed understanding of these needs is essential if the public and private sectors are to partner effectively to develop and execute initiatives to meet the full spectrum of cyber security skills requirements across our economy.

> **"Australia may need almost 18,000 additional cyber security workers by 2026 for the sector to harnesses its full growth potential[12]."**

The cyber skills gap

11%

of cybersecurity professionals around the world are women

Source: Global Information Security Workforce Study: Women in Cybersecurity 2017[18]

18,000

more Australian cyber security workers needed by 2026

Source: AustCyber 'Australia's Cyber Security Sector Competitiveness Plan 2018'[19]

The Schools Cyber Security Challenges

The Schools Cyber Security Challenges are practical resources for teachers to support the teaching of cyber security principles, aligned to the federal Digital Technologies Curriculum. The Challenges also aim to inspire students to consider careers in cyber security, featuring videos of real-life cyber security professionals describing their own work and career paths. As of October 2019, 35,000 students and 2,100 teachers had signed-up for the challenges.

The Challenges are aimed at high school students, but a second phase to be launched later in 2019 will also target year 5 and 6 pupils. The challenges begin with broad information security and privacy topics, but become increasingly specialised, covering subjects such as web application security, cryptography, and network security. The program also includes roadshows, aimed at helping teachers deliver the challenges in the classroom.

Building the cyber skills pipeline is not a competitive space and the Challenges are a great example of what can be achieved when industry partners, academia and government work together. The Schools Cyber Security Challenges were developed by the Australian Computing Academy at the University of Sydney, in partnership with AustCyber, ANZ, BT, Commonwealth Bank, National Australia Bank, and Westpac.

Cyber security education in schools

Teaching cyber safety in primary schools

We believe that Federal and State Governments should include 'cyber safety' principles in curriculums for primary school pupils. Whilst children are in many ways growing up as 'digital natives', they also need to learn how to keep themselves safe and secure online.

Teaching cyber security in high schools

Encouraging high school children to consider careers in computing generally, and in cyber security specifically, is a core component of securing the cyber skills pipeline. Introducing cyber security education to schools encourages diversity in the industry and generally raises Australians' cyber security awareness.

We commend the Commonwealth Government for including cyber security in the Digital Technologies curriculum for students in Years 9 and 10. CommBank has been extremely proud to work with the University of Sydney's Australian Computing Academy and industry partners, with support from AustCyber, to develop the Schools Cyber Security Challenges. These challenges complement and expand on the Digital Technologies curriculum, providing resources through which teachers can help their students learn cyber security principles (see text box "The Schools Cyber Security Challenges").

We would encourage the continued evolution of high school curriculums to emphasise a holistic approach that develops digital and cyber capability, including online safety, and inspires students to consider a career in cyber security. Successful execution of an engaging, holistic digital curriculum will build knowledge and capabilities, and equip future generations with the skills required to participate fully in the digital economy.

We would also encourage curriculums to emphasise the positive and inspiring 'purpose' of a career in cyber security, demonstrating how cyber security makes people, and our future, both safer and more prosperous. Research suggests that millennials want to work for businesses that match their values and that businesses should have a genuine purpose[20] – we anticipate that the emerging generation will continue this trend.

Addressing the gender imbalance

The so-called STEM subjects (Science, Technology, Engineering and Mathematics) are the foundations on which cyber skills are built. CommBank would strongly support sustained Government focus on encouraging the study – especially by female students – of STEM in schools. Intervention at this stage is absolutely necessary if we are to shift the dial on the current estimate that only 11% of the current global cyber workforce is female.[21] The percentage of female students enrolling in Year 12 Information and Communications Technology (ICT) and Design and Technology in 2017 was 26.3%, against 39.4% of male students – and this gap has widened since 2010.[22] Significant work is required if we are to reverse this trend, including taking steps to remove implicit bias such as by highlighting female STEM role models. We acknowledge the Government's very positive step of developing a "Decadal Plan for Women in STEM"[23] and the delivery of the Girls in STEM Toolkit.[24] We would encourage Government to ensure this plan is well-supported and resourced throughout its course, and look forward to seeing regular reporting on its results.

Teaching cyber security at universities

Cyber security curriculums

Australia's cyber security skills gap cannot be addressed unless our universities are producing sufficient graduates equipped with the skills required by industry. However, this is not simply a matter of numbers – we will never have enough STEM graduates to solve the problem through people alone. Innovative advances in technology, processes, and thinking are also required. Accordingly, it has been heartening to see more universities working closely with industry partners to develop their curriculums and to benefit from industry expertise in the delivery of their courses (see for example the "University of New South Wales SECedu Program" text box below).

Currently, there is global dialogue around "curriculum standardisation" for cyber security. We question whether this is the optimum approach for Australia. Australian universities are each producing different kinds of cyber experts, and the future will require a diverse mix of individuals. However, we do strongly encourage universities to create a "knowledge network" that would enable students to study across institutions, taking advantage of their relative strengths. We also recommend the Australian Government investigate setting challenges and projects that require students from multiple universities to cooperate (such as the Cyber Security Challenge Australia, see the text box on previous page).

The University of New South Wales SECedu Program

In 2015, CommBank invested $1.6 million to co-develop SECedu, a cyber security specialisation within the Computer Science degree at University of New South Wales. Subjects include offensive security, web application security and digital forensics. CommBank cyber security professionals also provide expertise and 'real world' insight to the students through lectures and course content. Graduates of SECedu have joined CBA and are already making a valuable contribution to our Cyber Security team.

A multi-disciplinary approach with solid technical foundations

We believe that the development of innovative cyber defences in Australia will require graduates with a solid grounding in computer science: the mathematical principles that underpin computing, as well as skills such as hardware and assembly language programming. We note with concern a trend for some Australian universities to move away from computer science degrees towards degrees in information technology that focus on how to effectively connect, use, and manage complex integrations of existing technology.

Cyber security is not, and never was, a matter of technology alone. Cyber security has always been about people, process and technology, and humans are all too often the weakest link in our cyber defences. If we are to think differently about cyber security and not repeat the mistakes of the past, cyber security experts of the future must be technical experts but also have a strong understanding of, and education in, adjacent “non-technical”, or “soft science” fields, including but not limited to:

- Social and Political Science;
- Finance and Economics;
- Risk Management; and
- Law.

Conversely, we note that the demand for cyber security skills in the modern workplace stretches beyond hands-on, technology-focussed professionals to include people who have not studied computer science, such as lawyers and compliance professionals, project managers, organisational change managers, etc. (see “Defining the cyber skills shortage” above). Accordingly, we would encourage universities to include cyber security modules in other disciplines that may end up producing the cyber security professionals of tomorrow, including law, psychology, criminology, business studies, etc.

Cyber Security Challenge Australia (CySCA)

CommBank recognises the expansion of the Government’s annual Cyber Security Challenge Australia (CySCA) as one of the successes of the 2016 Cyber Security Strategy. CommBank was proud to support these events, which attracted talent from Australian universities and TAFEs. CySCA became a highlight in many cyber security students’ calendars, creating a sense of national cyber security community, and providing a unique learning experience that helped drive skills development and engagement.

We acknowledge the resource demands of CySCA on industry sponsors and Government and would like to re-engage with ACSC and the other industry sponsors to resume the challenges in 2020, following their hiatus in 2019. We believe CySCA can be established to be more sustainable, inclusive and scaled. In particular, we would encourage smaller, more frequent and themed challenges.

Women in Cyber Mentoring Events

CommBank recognises the Women in Cyber Mentoring events, which bring together female university students participating in the CySCA events with women working in cyber security, as another of the successes of the 2016 Cyber Security Strategy. This initiative was another excellent example of the ACSC working with industry. To achieve greater impact, we suggest the following should be considered:

- The program should provide greater guidance and structure so that expectations of mentors and mentees are clear from the outset and mentors provide consistent levels of advice and support to mentees;
- The program should be de-coupled from CySCA, with an independent application process, so more young women are provided the opportunity to participate; and
- The inclusion of male champions of change as mentors or co-mentors.

Filling the Australian skills gap in the interim

It is a fact of life for Australian enterprises that the shortage of cyber security professionals in Australia requires the hiring of talent from overseas. CommBank recognises the need for Government and industry to partner more effectively and redouble their efforts to bridge the cyber skills gap, but also supports the continuation of the existing Temporary Skills Shortage visa regime that largely operates effectively in enabling Australian enterprises to source the cyber security talent they require from overseas.

The Government could consider including "cyber security professional" as one of the categories in the skilled occupation list to specifically recognise the need for cyber skills to help secure our digital economy.

Diverting at-risk youth from cyber crime

Disaffected, tech-savvy youth are at risk of falling into cyber crime, either of their own volition or through being recruited by cyber criminals. CommBank recommends that the Government consider establishing an intervention program to guide young people at risk of being drawn into cyber crime towards positive career alternatives in the cyber security industry. We note that the UK's National Crime Agency and Regional Organised Crime Units have developed a program of intervention days, which could provide a useful model. This program aims to teach young people about the law and ethics that surround activities such as hacking and to encourage them to think positively about cyber security roles in the legitimate economy.[25]

Recommendations to Government

- We recommend the Government commissions and publishes research that identifies in detail the shortage in our national cyber security workforce across disciplines and career stages.
- Federal and State Governments should include cyber safety in primary school curriculums, recognising that staying safe on-line is now a foundational life skill.
- We recommend the evolution of state and federal high school curriculums that adopt a holistic approach to cyber security and safety: building digital and cyber security capability, encouraging online safety, and inspiring students to consider a career in cyber security.
- We recommend that Government increase the focus on the study of STEM subjects (Science, Technology, Engineering and Mathematics) in school, particularly by female students, to provide the foundations on which cyber skills are built and help address the gender imbalance in the cyber security industry.
- The ACSC should re-engage industry partners to develop imaginative proposals for resuming the Cyber Security Challenges Australia for university and TAFE students in 2020, placing the challenges on a sustainable footing that enables their scaling and continued success.
- We recommend the continued operation of the Temporary Skills Shortage visa regime insofar as it applies to employing cyber security professionals from overseas as an interim measure, pending Australia becoming self-sufficient in producing cyber security talent.
- The Government should consider including "cyber security professional" as one of the categories in the skilled occupation list of the Temporary Skills Shortage visa regime.
- The ACSC should resume the Women in Cyber Mentoring Events to help redress the gender imbalance in the cyber security industry and consider evolving this concept to increase its impact, including making participation independent from the Cyber Security Challenges Australia.
- The Government should consider establishing an intervention program to guide young people at risk of being drawn into cyber crime towards positive career alternatives in the cyber security industry, possibly looking to the UK's model for 'intervention days'.

"Cyber security is not, and never was, a matter of technology alone. Cyber security has always been about people, process and technology, and humans are all too often the weakest link in our cyber defences."

Building cyber awareness

Government and industry must align how they address cyber awareness, adopting an approach that empowers businesses and individuals with practical advice, avoids spreading fear, uncertainty and doubt, and engages the intended audiences.

To help build cyber aware small- and medium-sized businesses (SMBs), Government should combine its trusted voice with private sector expertise to address common pain points and provide practical technical advice that can be easily implemented. This approach must acknowledge the limited time and resources available to SMBs.

To help raise public awareness, Government and industry will need to identify the needs of different sectors of society, including children, young people, parents, and older Australians. Advice must be practical and empowering, and delivered through the channels that are best suited to each audience.

Building cyber-aware businesses

Small- and medium-sized businesses (SMBs) are the lifeblood of our economy. However, owners of SMBs are busy, with limited time and resources to spend on security. Sadly, for many SMBs, cyber security is not a priority until they become a victim of cyber crime. CommBank takes the security of its over 500,000 business customers very seriously, and many of our initiatives to improve cyber security awareness are available to any business, whether or not it banks with us (see "CommBank Initiatives" text box below). In an increasingly connected business environment, we adopt the philosophy that we all benefit from securing Australia's digital ecosystem.

How the public and private sectors can cooperate to build cyber-aware businesses

We commend the ACSC for its recent increased focus on raising cyber awareness amongst small businesses. We know from discussions with our business customers that Government is considered a trusted voice when it comes to cyber security advice. However, many small businesses struggle to meet the demands of the ACSC's Essential Eight Strategies to Mitigate Cyber Security Incidents.[30] The ACSC's Small Business Cyber Security Guide[31] goes some way to addressing this gap by explaining in simple language some of the key cyber security threats and the foundational security measures small businesses can take to make themselves more secure.

What makes this initiative particularly effective is the ACSC's cooperation with key technology providers to produce Step-by-Step Guides[32] for specific operating systems (iOS and Windows) and for Facebook to make the use of these technologies more secure. We strongly support the expansion of these guides to other technologies widely used by small businesses, which should include securing the applications and other tools offered by banks.

We support the ACSC in its ambition to provide further advice booklets for SMBs to help them secure their businesses and commend the ACSC's approach of seeking input from industry partners. In particular, we appreciate the ACSC's straightforward and jargon-free advice to SMBs that seeks to address shared pain points that can be difficult to tackle, such as "Cloud Computing Security Considerations" and "Assessing Security Vulnerabilities and Applying Patches". We note the volume of guidance that the ACSC has now published and suggest that this should now be organised by themes, as well as by date, on the ACSC website to help time-poor SMBs find what they need more quickly.

Leveraging opportunities to raise awareness

We believe there is an opportunity for Government and industry to identify key points in the lifecycle of an SMB at which they could be provided them with ‘best of breed’ awareness materials and advice. These materials could be from both Government and trusted industry partners – cyber awareness is not a competitive space. These trigger points could include: the registration of a business, when a business establishes a bank account, or engages key service business and professional service providers (telecommunications, accountants, etc.).

> **“In an increasingly connected business environment, we adopt the philosophy that we all benefit from securing Australia’s digital ecosystem.”**

SMBs and cyber crime

98%

of Australian businesses are defined as SMBs

Source: Australian Small Business and Family Business Ombudsman Small Business Counts report (2019)[26]

43%

of reported data breaches in 2018 involved small businesses victims

Source: Verizon 2019 Data Breach Investigations Report[27]

1 in 4

Australian small businesses fell victim to cyber crime in 2017

Source: Norton 2017 SMB Cyber Security Survey, Australia[28]

87%

of SMBs would like resources or tools to help reduce their exposure to cyber crime

Source: NSW Small Business Commissioner, Cyber Aware: Report into the Perceptions of, attitudes to and preparedness for Cybercrime amongst Australia’s small and medium-sized enterprises (2017)[29]

CommBank initiatives to improve cyber security awareness in small- and medium-sized businesses

CommBank is proud of the resources and services it provides to its small- and medium-business customers to help them improve their cyber security. We also make some high-quality cyber security resources available to any organisation as part of our commitment to securing the Australian digital ecosystem.

Cyber awareness initiatives for business customers

- Over the past 12 months CommBank has provided face-to-face cyber security education sessions across the country that have been attended by over 4,400 people.
- Session attendees were from a variety of sectors including: not-for-profit organisations; rural and agricultural businesses; tertiary and secondary education; professional services; insurance; and local government.

Resources available to any organisation

- In 2019, CommBank launched its 'Better for You' campaign, which includes an online portal[33] where organisations can access a free cyber awareness eLearning module, known as 'Cool, Calm and Connected'. The module, originally based on CommBank's own training for its staff, aims to help organisations promote safer online behaviour by educating their employees.
- CommBank also publishes 'Signals'[34], a quarterly publication that aims to inform small- and medium-sized businesses what they can do to protect themselves from some of the attack trends that CommBank's own Cyber Security Centre observes. Recent topics have included business email compromise, phishing, and the concept of zero-trust.

Building a cyber-aware community

Stay Smart Online

The ACSC's annual "Stay Smart Online" week has become a fixture in Australia's cyber security calendar and is an excellent example of how government and businesses can work together to raise cyber security awareness. Stay Smart Online week unites messaging from government and participating businesses (including banks, telecommunications companies, Australia Post and major retailers) under one banner, with a consistent theme e.g. the 2019 campaign's theme was "Reverse the threat of cyber crime". This concerted approach means that every Australian adult using online services is likely to be exposed to cyber security advice during the week from at least one public or private sector organisation.

Step-by-step guides aimed at individuals

We believe that individuals would benefit from ACSC and/or the Office of the e-Safety Commissioner developing 'step-by-step' guides to securing specific technologies, similar to those produced by the ACSC for small businesses (see above), and adopting a similar model of partnership between Government and the technology-providers. These guides could provide clear, practical guidance to individuals on how to improve their cyber security and cyber safety when using specific, popular technologies e.g. implementing multifactor authentication, locking down privacy settings on social media.

Older Australians

As public and private sector services are increasingly available through online channels and some services become available only online, older Australians who may not be prolific users of the internet need to learn how to stay safe online and protect themselves. Unfortunately, we are aware that some cynical cyber criminals deliberately target older Australians.

This advice needs to be delivered in an audience friendly way and through appropriate channels. At CommBank we run in-branch "Staying Safe Online"[35] sessions to provide our customers with foundational skills to safely use online banking, such as identifying phishing and email scams. These sessions are open to all CommBank customers, but we have found that this face-to-face approach is particularly helpful to older Australians who may be less inclined to seek advice from online sources.

We would encourage Government as a key trusted voice to work with industry partners to help deliver more advice to older Australians on cyber safety and cyber security in ways that best suit their needs: including through face-to-face sessions and printed guides.

Parents and young people

It can be a challenge for parents to discuss confidently with their children how they use the Internet and risks to which they may be exposed. Similarly, it can be difficult for young people to know where to find reliable information on their own cyber safety. The ThinkUKnow program[36] is a partnership between police and industry partners, including CommBank, to bridge the knowledge gap between adults and young people so that everyone has an understanding of the roles they play and what they can do if something goes wrong online, including how to report abuse. We are experiencing high demand for this type of practical education, which is run on a volunteer basis. We would encourage increased government resources and industry participation to scale this program and place it on a sustainable footing.

Media campaigns

We would encourage Government to increase investment in public awareness of personal and business cyber security and safety, including through media campaigns. The ideal campaign would distil advice on cyber security and safety into a message as simple as the 'Slip, Slop, Slap' campaign for skin cancer devised by Cancer Council Victoria in 1980, which is often held up as a model.[37] However, we acknowledge the immense challenge of reducing as complex a subject as cyber security advice into such a concise and memorable formula.

We suggest a successful media campaign must have the following attributes:

- It should catalyse a cultural shift towards cyber security, similar to that which occurred in workplace Occupational Health and Safety during the 1980s and 1990s in Australia. Not unlike cyber security, the situation at the time was multi-faceted and complex, and the solutions required to create the cultural shift towards health and safety were several and varied. However, change was driven by an overarching motivation to 'come home safe at the end of the day'. We believe we need a similar overarching message, underpinned by the actions and activities discussed throughout this submission, which serves as a call to action to ensure the digital wellbeing of all Australians.
- It must avoid spreading fear, uncertainty and doubt. Cyber security should be represented as a challenge that individuals or businesses are capable of addressing, not as an impenetrable technical subject or as a hopeless match against a faceless, hoodie-wearing technical genius. We have seen examples such as the entertaining Dubai police "It wasn't me" campaign[38], which takes a different tack entirely: using humour to make cyber security an approachable subject.
- It should empower individuals by offering specific, practical advice on how to protect themselves. The 'Slip, Slap, Slop' campaign is a great example of this, as is New South Wales Road Safety 'Plan B' campaign[39], which sought to reduce drink driving by encouraging drivers to make simple, positive behavioural choices.

Recommendations to Government

- The ACSC should work with industry partners to develop more 'Step-by-Step' guides, aimed at small businesses, and providing simple, practical advice on how to secure specific, widely used technologies.
- We would suggest that the ACSC organises the materials available for download on its website by theme as well as date for easier navigation by time-poor small- and medium-sized businesses (SMBs).
- We recommend that Government should identify key points in the SMB lifecycle (e.g. when registering a business) as opportunities to provide SMBs with 'best of breed' cyber security awareness materials from both Government and private sector sources.
- We recommend Government continues to work with industry partners to raise cyber security awareness through aligned messaging over multiple channels during the annual "Stay Smart Online Week".
- We suggest the ACSC and/or eSafety Commissioner's office develop 'step-by-step' guides to help individuals to secure widely used technologies and protect their personal data.
- We encourage Government to work with industry partners to deliver more advice to older Australians on cyber safety and cyber security in ways that best suit their needs - including through face-to-face sessions and printed guides.
- We encourage increased government resources and industry participation to scale the ThinkUKnow cyber safety program (aimed at parents and young people) and place it on a sustainable footing.
- We recommend Government develops a media campaign that helps catalyse a cultural shift towards cyber security by empowering and engaging individuals with practical advice, and avoids spreading fear, uncertainty and doubt.

Ensuring our legal and regulatory framework supports cyber security

We believe Australia's laws and regulations should drive improvements in cyber security standards, whilst avoiding stifling innovation. To maintain Australia's position as an attractive place to develop and invest in technology, the Government must actively engage the technology community on policy and legislation that could impact our technology industries. Legislation must support the security of supply chains, including by holding software and hardware developers and manufacturers responsible for quickly remediating vulnerabilities. We also need a well-designed regulatory framework that focuses on raising standards and avoids imposing duplicative reporting accountabilities to government agencies.

Improving supply chain security

Identification, disclosure and remediation of vulnerabilities

As discussed in "Our view of the Australian threat environment", Australia has a more centralised IT provider community than many comparable jurisdictions, exposing the nation to greater risk when one of these central providers is compromised. Many Australian businesses and institutions also use common software and hardware, resulting in further concentration risk. Accordingly, it is important that our legal framework helps ensure vulnerabilities in widely used or critical software and hardware are quickly identified and remediated.

We recommend that Government consider whether more could be done to secure Australian supply chains by introducing or strengthening legal provisions and mechanisms that:

- Encourage or compel hardware and software companies to take reasonable and timely steps to remediate critical vulnerabilities of which they become aware; and
- Create a process by which security researchers or customers of hardware and software companies are able to share vulnerabilities that they identify with an appropriate government agency without fear of legal action by the vendor. The government agency could then take appropriate steps to encourage remediation by the vendor and, in cases where the vendor is unwilling to take prompt remediation steps, notify other customers of the vulnerability.

Creating a legal environment that supports digital innovation

A strong Australian cyber security industry is most likely to develop and thrive in the context of a broader, healthy technology industry. Accordingly, we would encourage Government to consult with the technology community when developing legislation that could impact technology innovation and the cybersecurity sector. This dialogue is essential to help avoid unintended consequences and misunderstandings, which could undermine confidence in Australia as a tech-friendly environment. In this context, we would encourage the Government to take further steps to those taken to date[40] to clarify the intention and operation of the Assistance and Access Act, which members of the Australian technology industry have cited as potentially making Australian technology less attractive in overseas markets.[41]

Regulatory harmonisation

The local and global regulatory environment has become increasingly complex as it seeks to protect the data, privacy and security of individuals, companies and governments. In recent years, we have seen a significant increase in the volume and complexity of regulatory standards in the jurisdictions in which CommBank operates as well as those imposed by domestic regulators. Like many Australian companies that operate globally, this increased level of regulation gives rise to an increased compliance burden.

Particular examples of where harmonisation of domestic regulation would benefit Australian organisations include:

- Co-ordinated incident reporting regime: There are now a number of reporting obligations pursuant to a number of regulatory regimes (e.g. mandatory data breach notification under the Privacy Act, Prudential Standard CPS 234, the Banking Executives Accountability Regime). This results in unnecessary duplication as notification for the same incident is required by multiple local regulators and/or government departments. There may be an opportunity for a coordinated government regulatory regime in relation to cyber security that could facilitate simpler cyber incident reporting.
- Notification to consumers: As the operation of the Australian mandatory data breach notification regime under the Privacy Act matures, Australian businesses would benefit from further guidance to ensure notifications to affected customers and contacts are consistent, meet the needs of affected individuals, and avoid multiple uncoordinated notifications where several organisations are involved in a single incident.

To support Australian companies to continue operating globally whilst maintaining high standards of cyber security, CommBank encourages harmonisation of cyber security standards where possible. For example, the timeframes and thresholds for notifications to affected customers or to regulatory bodies vary across jurisdictions, providing another level of process complexity for international businesses.

Recommendations to Government

- We recommend that Government considers introducing or strengthening legal provisions and mechanisms that encourage or compel hardware and software companies to take reasonable and timely steps to remediate critical vulnerabilities of which they become aware.
- We recommend that Government considers creating a process by which security researchers or customers of hardware and software companies can share vulnerabilities that they identify with an appropriate government agency, which is empowered to take appropriate steps to encourage remediation by the vendor.
- We encourage Government to consult with the technology community when developing legislation that could impact technology innovation and the cybersecurity sector to avoid unintended consequences and misunderstandings that could undermine confidence in Australia as a tech-friendly environment.
- We encourage Government to take further steps to clarify the intention and operation of the Assistance and Access Act, which members of the Australian technology industry have cited as potentially making Australian technology less attractive in overseas markets.
- We encourage Government to coordinate the regulatory regime to avoid the need for businesses to make duplicate notifications to multiple regulators and/or government departments in relation to the same incident or issue.
- We encourage Government to issue further guidance on the mandatory breach notification regime to ensure notifications of affected customers and contacts are consistent, meet the needs of affected individuals, and avoid multiple uncoordinated notifications where several organisations are involved in a single incident.
- We encourage Government to pursue international harmonisation of cyber security standards where possible to make it easier for Australian companies to operate globally, including seeking common timeframes and thresholds for notifications to affected customers or to regulatory bodies across jurisdictions.

Summary of recommendations

The Australian cyber threat environment

1. The Government should focus on reducing cyber crime to help prevent the diversion of funds into the illegitimate economy and to maintain public trust in the Australian digital ecosystem. This will require close cooperation between government and industry to increase public awareness of cyber crime and create technical barriers to make life harder for cyber criminals.
2. The rapidly changing Australian threat environment and the increasing interconnectedness of supply chains in our digital economy make it imperative that Government and industry improve their cooperation in sharing cyber threat intelligence in a timely and efficient manner.

The role of Government in addressing the most serious threats to Australian institutions and businesses

3. Government should work with industry partners to develop a clear framework that provides guidance to organisations on when to engage the ACSC in a cyber security incident, the assistance the ACSC can offer, and the consequences for not engaging.
4. The ACSC should work with industry partners and across government, including regulators, to develop a model for responding to a major cyber incident that prioritises understanding and containing the attack.
5. Government should work with major industries and critical national infrastructure providers to develop and exercise response plans and scenario playbooks for responding and recovering from a major cyber attack that targets one or more industries simultaneously.
6. The ACSC should be resourced to enable it to produce and disseminate timely and actionable threat intelligence based on its assessment and analysis of the major incidents with which it is involved.
7. ACSC should consider resuming publication of the annual ACSC Threat Report (or a more frequently published regular trend report), as this reporting filled a gap in coverage with its focus on the Australian threat environment.
8. Government should seek ways to accelerate the declassification of cyber threat intelligence and its distribution to industry partners, noting the success of the UK National Cyber Security Centre's 'IOC Machine' initiative to automate some of this process.
9. Government should consider resourcing the ACSC to act as a central hub for the collection and dissemination of cyber threat intelligence from trusted industry partners.
10. Government should establish a secure channel for the exchange of cyber security information and intelligence between government and industry.
11. We recommend Government conducts a regular survey (e.g. every two years) of leading companies' cyber posture, governance and capabilities, the results of which are reported with analysis and comment from the ACSC on global better practice.
12. Government should continue to fund and support the JCSCs to provide focal points for the cyber security community, hosting information exchanges and events that help organisations and individuals across the Australian economy to be more secure.

Addressing the Cyber Skills Gap

13. We recommend the Government commissions and publishes research that identifies in detail the shortages in our national cyber security workforce across disciplines and career stages.
14. Federal and State Governments should include cyber safety in primary school curriculums, recognising that staying safe on-line is now a foundational life skill.

15. We recommend the evolution of state and federal high school curriculums that adopt a holistic approach to cyber security and safety: building digital and cyber security capability, encouraging online safety, and inspiring students to consider a career in cyber security.

16. We recommend that Government increase the focus on the study of STEM subjects (Science, Technology, Engineering and Mathematics) in school, particularly by female students, to provide the foundations on which cyber skills are built and help address the gender imbalance in the cyber security industry.

17. The ACSC should re-engage industry partners to develop imaginative proposals for resuming the Cyber Security Challenges Australia for university and TAFE students in 2020, placing the challenges on a sustainable footing that enables their scaling and continued success.

18. We recommend the continued operation of the Temporary Skills Shortage visa regime insofar as it applies to employing cyber security professionals from overseas as an interim measure, pending Australia becoming self-sufficient in producing cyber security talent.

19. The Government should consider including "cyber security professional" as one of the categories in the skilled occupation list of the Temporary Skills Shortage visa regime.

20. The ACSC should resume the Women in Cyber Mentoring Events to help redress the gender imbalance in the cyber security industry and consider evolving this concept to increase its impact, including making participation independent from the Cyber Security Challenges Australia.

21. The Government should consider establishing an intervention program to guide young people at risk of being drawn into cyber crime towards positive career alternatives in the cyber security industry, possibly looking to the UK's model for 'intervention days'.

Building cyber awareness

22. The ACSC should work with industry partners to develop more 'Step by Step' guides, aimed at small businesses, and providing simple, practical advice on how to secure specific, widely used technologies.

23. We would suggest that the ACSC organises the materials available for download on its website by theme as well as date for easier navigation by time-poor small- and medium-sized businesses (SMBs).

24. We recommend that Government should identify key points in the SMB lifecycle (e.g. when registering a business) as opportunities to provide SMBs with 'best of breed' cyber security awareness materials from both government and private sector sources.

25. We recommend Government continues to work with industry partners to raise cyber security awareness through aligned messaging over multiple channels during the annual "Stay Smart Online Week".

26. We suggest the ACSC and/or eSafety Commissioner's office develop 'step-by-step' guides to help individuals to secure widely used technologies and protect their personal data.

27. We encourage Government to work with industry partners to deliver more advice to older Australians on cyber safety and cyber security in ways that best suit their needs - including through face-to-face sessions and printed guides.

28. We encourage increased government resources and industry participation to scale the ThinkUKnow cyber safety program (aimed at parents and young people) and place it on a sustainable footing.

29. We recommend Government develops a media campaign that helps catalyse a cultural shift towards cyber security by empowering and engaging individuals with practical advice, and avoids spreading fear, uncertainty and doubt.

Ensuring our legal and regulatory framework supports cyber security

30. We recommend that Government considers introducing or strengthening legal provisions and mechanisms that encourage or compel hardware and software companies to take reasonable and timely steps to remediate critical vulnerabilities of which they become aware.

31. We recommend that Government considers creating a process by which security researchers or customers of hardware and software companies can share vulnerabilities that they identify with an appropriate government agency, which is empowered to take appropriate steps to encourage remediation by the vendor.

32. We encourage Government to consult with the technology community when developing legislation that could impact technology innovation and the cybersecurity sector to avoid unintended consequences and misunderstandings that could undermine confidence in Australia as a tech-friendly environment.

33. We encourage Government to take further steps to clarify the intention and operation of the Assistance and Access Act, which members of the Australian technology industry have cited as potentially making Australian technology less attractive in overseas markets.

34. We encourage Government to coordinate the regulatory regime to avoid the need for businesses to make duplicate notifications to multiple regulators and/or government departments in relation to the same incident or issue.

35. We encourage Government to issue further guidance on the mandatory breach notification regime to ensure notifications of affected customers and contacts are consistent, meet the needs of affected individuals, and avoid multiple uncoordinated notifications where several organisations are involved in a single incident.

36. We encourage Government to pursue international harmonisation of cyber security standards where possible to make it easier for Australian companies to operate globally, including seeking common timeframes and thresholds for notifications to affected customers or to regulatory bodies across jurisdictions

Endnotes

1. Office of the Australian Information Commissioner, Notifiable Data Breaches Statistic Report 1 April to 30 June 2019
2. Mimecast, The State of Email Security 2019
3. Australian Bureau of Statistics, Household Use of Information Technology 2016-17
4. Group IB, High Tech Crime Trends, 2018
5. ACCC, Targeting scams: report of the ACCC on scam activity 2018
6. Agari, BEC goes mobile as cyber criminals turn to SMS, 19 March 2019
7. SANS, Newsletter: CEO Fraud, July 2016
8. Forbes, A Voice Deepfake Was Used To Scam A CEO Out Of $243,000, 3 September 2019
9. An example would be how some scammers would deliberately use unsophisticated fraudulent emails to attract the most gullible victims from a large set of potential targets: https://www.microsoft.com/en-us/research/publication/why-do-nigerian-scammers-say-they-are-from-nigeria/
10. The Australian Business Review, One call all it takes for superannuation savings to vanish, 30 October 2019
11. ACCC, Targeting scams: report of the ACCC on scam activity 2018
12. Accenture, 2019 Cost of Cyber Crime Study
13. Federal Bureau of Investigation, Business E-Mail Compromise The 12 Billion Dollar Scam, 12 July 2018
14. Federal Aviation Administration, Fly the Aircraft First, 2018
15. UK National Cyber Security Centre Annual Review 2019, p52
16. Website of the National Council of Information Sharing and Analysis Centers
17. AustCyber, Sector Competitiveness Plan, 2018
18. Frost & Sullivan, Global Information Security Workforce Study: Women in Cybersecurity, 2017
19. AustCyber, Sector Competitiveness Plan, 2018
20. See, for example: American Express, Redefining the C-Suite: Business the millennial way, 29 November 2017
21. UNSW BusinessThink, Why bringing on more cyber women is a matter of national security, 17 October 2018
22. Australian Government Department of Industry, Innovation and Science, Advancing Women in STEM, April 2019
23. Australian Government Department of Industry, Innovation and Science, Advancing Women in STEM, April 2019
24. Australian Government Department of Industry, Innovation and Science, The Girls in STEM Toolkit: www.thegist.edu.au
25. Cyber Security Challenge UK, National Crime Agency Intervention Days
26. ASBFEO, Small Business Counts: small business sin the Australian economy, July 2019
27. Verizon, 2019 Data Breach Investigations Report, 8 May 2019
28. Norton, SMB Cyber Security Survey 2017
29. NSW Government, Cyber Aware Report, November 2017
30. ACSC, Essential Eight Explained, April 2019
31. ACSC, Small Business Cyber Security Guide, October 2019
32. ACSC publications list: https://www.cyber.gov.au/publications
33. CommBank Secure webpage: https://www.commbank.com.au/support/security.html
34. CommBank Secure webpage: https://www.commbank.com.au/support/security.html
35. CommBank, Helping you stay safe online
36. ThinkUKnow website: www.thinkuknow.org.au
37. CIO, In search of a Slip, Slop, Slap for cyber security, 4 October 2017
38. Emirates NBD, 'It Wasn't Me' (hosted by YouTube)
39. Transport for NSW, Centre for Road Safety, 'Plan B'
40. For example, Australian Government Department of Home Affairs, Assistance and Access: Common myths and misconceptions, 2019
41. News.com.au, 'Australian companies are already losing': Tech industry takes aim at controversial internet encryption bill, 12 February 2019

CommonwealthBank