Commonwealth Bank

2023-2030 Australian Cyber Security Strategy

Response to Discussion Paper

April 2023

Public

Executive Summary

The Commonwealth Bank of Australia (CBA) welcomes the opportunity to participate in the Australian Government's 2023-2030 Australian Cyber Security Strategy (the Strategy) consultation.

CBA agrees with the view in the Minister's foreword that Australia's framework of policies, law and frameworks need to evolve to keep pace with the challenges presented by the digital age.[1] The development of the Strategy provides an opportunity to build a regulatory system and optimise policy settings to achieve the Australian Government's objective of being the world's most cyber secure country by 2030. To achieve this goal, it will take a unified approach between government, business, and the community to enhance our collective cyber resilience.

CBA believes the following actions should be addressed to optimise the cyber regulatory framework:

- Take steps to address duplicative and overlapping regulatory obligations and gaps in the current system;
- Establish a single regulatory body at the heart of the cyber regulatory regime empowered with authority and leadership to promote coordination with industry, during cyber-incidents;
- Enable organisations to contact the Australian Cyber Security Centre (ACSC) in a way that does not constitute a formal notification if they suspect they are experiencing a potential cyber incident but are yet to confirm this;
- Promote the adoption of the Australian Government's Digital Identity framework to reduce the opportunity for unauthorised sharing of personal information, identity theft and fraud;
- Optimise national frameworks such as the Trusted Information Sharing Network (TISN) to streamline information flows, and allow for a more agile response to cyber incidents, and
- Implement a single reporting portal sitting within a Government body that can support incident response.

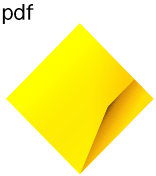
Key areas where Government can play a pivotal role beyond the current regulatory and operational framework in response to cyber incidents include:

- Strengthen mechanisms to coordinate and facilitate engagement and action in real time during attacks;
- Utilise the offensive capabilities of Government to interrupt malicious threat actors.
- Design a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda, and
- Further our international engagement on cyber security issues to benefit from use of emerging technology, skills development and transfer, and current understanding of the cyber threat landscape, particularly as it evolves in the Asia-Pacific

On balance, CBA would be supportive of a Cyber Security Act if it had a simplifying impact in terms of aligning existing regulation. CBA welcomes the immediate development of cyber exercises, as part of the rollout of a National Cyber Exercise series as recently outlined by the Minister. CBA supports the view that these should not wait until the Strategy is finalised.

In the development of the Strategy, CBA encourages the Government to:

[1] Australian Government (2023), 2023-2030 Australian Cyber Security Strategy Discussion Paper, Minister Foreword, p4 https://www.homeaffairs.gov.au/reports-and-pubs/files/2023-2030_australian_cyber_security_strategy_discussion_paper.pdf



- Take the existing regime (including privacy laws) and identify how this may be simplified, not necessarily expanded, when approaching regulatory reform in relation to the Security of Critical Infrastructure (SOCI) Act, and
- Align the outcomes of the current consultation with that of the Privacy Act Review, to ensure harmony amongst the various regulatory frameworks and avoid introducing duplications or competing obligations.

CBA does not support new and specific obligations on company directors to address cyber security risks and consequences. It is unnecessary to develop additional specific cyber-related obligations for company directors as the current principles-based approach to defining directors' duties (that a director must act with reasonable care and diligence) is sufficient.

CBA would welcome the opportunity to further discuss this submission and provide any additional insights towards the development of the Australian Government's 2023-2030 Cyber Security Strategy.

1. Enhancing and harmonising regulatory frameworks (questions 1-2)

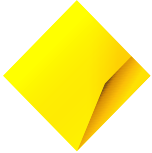
i. General

To enhance cyber resilience across the digital economy, the Government must consistently assess the full suite of government systems and regulatory obligations in-force, to ensure they are fit for purpose.

The development of the Strategy provides an opportunity to consider a comprehensive review of the inconsistencies and the creation of an overarching cyber regulatory framework. CBA believes the following actions should be prioritised:

a) Embark on a process of mapping out, and clearly demarcating roles and responsibilities for different areas of cyber security and resilience policy among the various agencies and government bodies that are currently involved in the system. This would help reveal duplicative and overlapping regulatory obligations and identify gaps in the system.
b) Conduct national cyber simulations involving large players across different sectors of the economy and regulatory bodies to draw out current limitations and illustrate where improvements can be made. CBA welcomes recent announcements from the Government in relation to the rollout of a national cyber exercise series, where Government will systematically and frequently exercise with entities covered by SOCI on a sectoral and cross-sectoral basis.[2]
c) Establish a single regulatory body at the heart of the cyber regulatory regime empowered with authority and leadership to promote coordination with industry, during cyber-incidents. This regulator would collaborate with, and coordinate a response on behalf of, all government and regulatory agencies.
d) Enable organisations to contact the ACSC if they suspect they are experiencing a potential cyber incident in a way that would not constitute a formal notification. By way of example, in this environment, organisations could confidentially contact ACSC to seek advice, intelligence, or additional directions.
e) Promote the adoption of the Australian Government's Digital Identity framework to restrict oversharing of personal information and limit the risks of identity theft and fraud.

[2] https://www.theaustralian.com.au/nation/politics/firms-called-up-for-cyber-war-games/news-story/1826124adcfdcc9b08207b50ca0305ab



f) Align the outcomes of this consultation with that of the Attorney General Department's (AGD) Privacy Act Review to ensure that guidance and laws around the security of data (including personal information) are harmonised.

We believe the above recommendations would improve the timeliness, effectiveness and efficiency of cyber-related regulatory activity and reduce compliance costs for industry.

ii. *Standards*

The current legislative model is complex, which makes standards hard to find, interpret and to apply.

Overly prescriptive legal requirements can result in compliance at the minimum, rather than facilitating a dynamic response capability that can respond to evolving cyber threats. CBA supports a model common in other context, where powers are allocated through legislation, but detail as to how these laws apply is set through regulatory guidance, relative to specific characteristics of the industry or sector,. For example, powers provisioned under the Banking Act are then enforced through APRA's prudential standards (e.g. CPS 234 Information Security standard). Designing standards in a more digestible state is a key enabler for compliance.

iii. Security of Critical Infrastructure Act

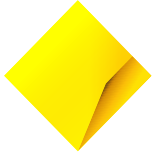
The discussion paper asks whether further reform to SOCI is required, to expand the existing definitions of 'critical assets' to include 'customer data and systems'.

CBA encourages Government to take into account the existing regime (including privacy laws) and how this may be simplified, not necessarily expanded, when approaching regulatory reform and how large-scale organisations operate in practice. We also suggest that the Government consider how proposed reforms under the Privacy Act Review may duplicate the existing regime. For example Proposal 4.6 of the AGD's Privacy Act Review Report proposes to extend the scope of obligations under Australian Privacy Principle 11.1 to de-identified information.[3] However, we note that such data (including personal information) as used by banks is already regulated under CPS 234 and the Security of Critical Infrastructure regime.[4] CBA encourages the Government to align outcomes of the current consultation with that of the Privacy Act Review, to ensure alignment among relevant regulatory frameworks and avoid introducing duplications or create competing obligations. As discussed further below, incident-reporting regimes should be aligned and simplified in an effort to minimise regulatory overlap when communicating details of a cyber-breach..

CBA believes that responsibility for reporting cyber incidents that affect customer data should be the responsibility of the customer-facing organisation and not an organisation that processes that data (and the data of a number of other clients). Without a clear purpose for the extension of the scope of the Act to customer data and systems, changes in this respect may increase the compliance burden without contributing to enhanced cyber resilience. For example, if the processor takes on regulatory accountability, this may introduce differences in opinion on how to respond to incidents. In our view, customer data is already protected by existing regulatory requirements applicable to customer facing organisations.

iv. Obligations of company directors

[3] https://www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf
[4] Department of Home Affairs, 'Critical Infrastructure: Changes to current regulation, 23 March 2023 (Available here).



CBA does not support new and specific obligations on company directors to address cyber security risks and consequences. Cyber is one of many emerging and existing material risks, such as climate change, that directors must take into account when carrying out their existing duties.

In our view it is unnecessary to develop additional specific cyber-related obligations for company directors, as the current principles-based approach to defining directors' duties, that a director must act with reasonable care and diligence, is sufficient. Section 180 of the Corporations Act makes clear that the degree of care and diligence required of directors is that which a reasonable person would exercise in the circumstances of the company and with the position and responsibilities of the relevant director.

The decision in *ASIC vs RI Advice Group Pty Ltd* indicates that company directors are required to consider cybersecurity risk oversight and disclosure obligations as part of their duties. The Australian Securities and Investments Commission (ASIC) has confirmed that the decision creates a requirement for AFS licensees to have adequate technological systems, policies and procedures in place to ensure sensitive consumer information is protected.[5] Organisations should take measures that are proportionate to the nature, scale and complexity of their organisation and the criticality and sensitivity of their operations. This includes reassessment of cybersecurity risks on an ongoing basis, based on threat intelligence and assessments of vulnerabilities.[6]

While the case concerned an Australian Finance Services Licence holder, it appears relevant for other entities subject to similar statutory obligations, such as APRA-regulated Authorised deposit-taking institutions (who are required to comply with CPS 234 (Information Security)), and Australian credit licensees under the National Consumer Credit Protection Act 2009 (Cth).

Rather than increasing specific director obligations, a more effective approach would be to further support director education and best-practice sharing mechanisms so that company directors can be as effective as possible in carrying out the cyber security aspects of their existing responsibilities.

v. Consideration of a Cyber Security Act

The discussion paper makes it clear that a package of regulatory reform is necessary to enhance Australia's cyber resilience, with specific reference made to the consideration of a new *Cyber Security Act*.

CBA understands that this legislation would seek to draw together cyber-specific obligations and standards across industry and government.

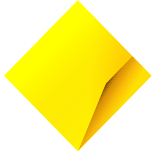
From the discussion paper, it is unclear whether the proposed Cyber Security Act would largely encompass all powers and obligations conveyed by the existing regime. On balance, CBA would be supportive of a Cyber Security Act if it had a simplifying impact in terms of aligning existing regulation.

vi. Ransoms

CBA notes the discussion paper's questions in relation to ransoms and extortion attempts noting that the Government may wish to take a position prohibiting the payment of ransoms on the basis that it may reduce or remove the ransom payment market in Australia.

CBA encourages some discretion for the payment of ransoms, as opposed to a complete prohibition. Whether a payment would be made depends on the exact circumstances and costs of the cyber incident.

[5] https://asic.gov.au/about-asic/news-centre/articles/what-a-federal-court-ruling-on-cybersecurity-means-for-afs-licensees/
[6] https://asic.gov.au/about-asic/news-centre/articles/cyber-risk-be-prepared/



Consistent with most countries, there is currently no express prohibition on the payment of a ransom amount in Australia. We note are aware that the OAIC and ACSC do not recommend that organisations pay ransom demands. This is also consistent with several countries (e.g. US, UK, EU and Singapore) where law enforcement and Government agencies strongly discourage the payment of ransoms.

CBA has followed the progress of the Ransomware Action Plan and Ransomware Payment Bills in Australia which, among other things, will introduce ransom reporting obligations. These proposed reporting obligations envisage that there would be circumstances in which a ransom could be paid and require notification of key information to the Government or law enforcement agencies.

The Government should clarify its position with respect to payment or non-payment of ransoms by companies and circumstances, which may constitute a breach of Australian Law. Currently, there are a variety of laws that may prohibit payment of a ransom to a particular threat actor, these include but are not limited to sanction laws, terrorism financing restrictions, money-laundering laws. These considerations create positive arguments for a 'safe harbour' immunity regime, to the extent that ransoms are permitted.

2. Strengthening Australia's international strategy on cyber security (questions 3-5)

Australia cannot, and does not, act in isolation in addressing cyber threats. CBA welcomes efforts to bolster Australia's international engagement on cybersecurity and agrees with the discussion paper that combined with domestic uplift and strengthened international leadership, this will enable Australia to address the challenges presented by the shifting cyber environment. This is becoming increasingly important as the digital economy becomes more global with commerce being conducted beyond borders and consumer data held offshore.

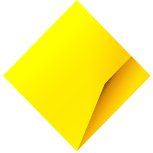
Placing Australia at the heart of international cyber engagement and collaboration positions Australia to benefit from use of emerging technology, skills development and transfer, and understanding the cyber threat landscape, particularly as it evolves in the Asia-Pacific.

CBA welcomes recent reporting noting that Australia's international and domestic cyber strategies will be integrated in the Strategy, with a renewed cyber diplomacy push seeking to make Australia the "partner of choice" for Pacific nations.[7]

To build regional cyber resilience, CBA encourages the Government to:

- Prioritise formal knowledge sharing arrangements between industry governments and their regulators that focus specifically on cyber resilience to identify the common concerns and work towards resolving those at industry and regional levels.
- Provide cyber training and financial support to aid the development of cyber skills in the Asia-Pacific region, particularly those where cyber resilience is low.
- Pursue 'mission' style delegations of cyber leaders to engage with local industry and the domestic regulators of our international partners.
- Conduct cross-border, cross-industry simulation exercises on plausible high impact scenarios.
- Promote inter-jurisdictional resource sharing such as exchange programs for students studying cyber related fields.

[7] International Cyber Strategy Rolls Into National Plan, https://www.innovationaus.com/international-cyber-strategy-rolls-into-national-plan/ 6 April 2023



3. Government delivery of cyber security best practice (questions 6-8)

CBA welcomes collaborative efforts between industry and government to enhance each other's collective cyber resilience.

Cyber simulations or exercises are an important component in building resilience, shared understanding, and promoting Government's ability to deliver cyber security best practice. As recently outlined by the Minister, cyber simulations or exercises build muscle memory in how to deal with a cyber-attack – and importantly can cover the types of incidents we have not yet experienced on a national scale – such as a lock-up of critical infrastructure or integrity attacks on critical data. CBA welcomes the immediate development of cyber exercises, as part of the rollout of a National Cyber Exercise series, and supports the view that Government should not await finalisation of the cyber strategy.[8]

As a further initiative to promote collaboration and build best practice, CBA would support the development of public-private exchange programs to ensure that both sides understand each other's perspective in assessing and responding to cyber threats. Such programs exist in the United States where the Department of Defence (DoD) have established the Cyber Information Technology Exchange Program (CITEP). The program enables DoD and private sector employees in the information technology and cybersecurity fields to participate in an exchange between the two sectors that seeks to enhance cybersecurity competencies and technical skills, share information, and bridge the culture gap between sectors.[9]

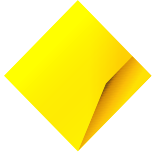
To promote open and transparent information sharing during a cyber-incident, CBA would welcome an explicit obligation of confidentiality upon the Australian Signals Directorate (ASD) and ACSC, as proposed in the discussion paper. Such an obligation would improve engagement with these government organisations at the critical stage of a cyber-incident, when focus must be on prioritising response and recovery, ahead of any related regulatory enforcement action.

In addition, CBA would support initiatives that improve information sharing between industry and government. Exchanging intelligence on current and emerging cyber threats from government entities who support organisations with incident response would also enhance the collective cyber defences of industry. For instance, practical instruments for consideration may include a register of known scam numbers and samples of Business Email Compromise (BEC) threats. CBA believe Government entities could play a leadership role in raising awareness of the technical details behind a cyber-incident such as the Tactics, Techniques and Procedures (TPP) and Indicators of Compromise (IOC).

4. Improving public-private mechanisms for cyber threat sharing and blocking (questions 9-10)

CBA agrees that if Australia is to lift and sustain cyber resilience and security, it must be an integrated whole-of-nation endeavour.

[8] Speech to Australia Strategic Policy Institute, Sydney Dialogue, Tues 4 April 2023 - https://minister.homeaffairs.gov.au/ClareONeil/Pages/aspi-sydney-dialogue-speech.aspx
[9] https://public.cyber.mil/wid/cdp/citep/



The discussion paper asks whether expanding the existing regime for notification of cyber security incidents (e.g. to require mandatory reporting of ransomware or extortion demands) would improve the public's understanding of the nature and scale of ransomware and extortion as a cybercrime type. CBA agrees that there is value in understanding the trends in cybercrime as it pertains to fraud management, however questions whether a requirement to report publicly on all cybercrime would assist the community, given the scale of the cyber threat landscape. Rather, CBA encourages government to continue to strengthen the value in the Australian Financial Crimes Exchanges (AFCX) as a platform for sharing cybercrime related fraud incidents whilst not over-reporting incident data that may lack context of environment or cause. AFCX has proven to be an effective platform for intelligence sharing on the latest cybercrime trends.

Any additional measures to enhance notifications to the public of cyber incidents should be aggregated and tied to tangible actions the public can take to better protect themselves. This might include information on what to do if customers believe they have been impacted by a cyber-incident and/or links to centrally offered services they can consume.

5. Supporting Australia's cyber security workforce and skills pipeline (questions 11-12)

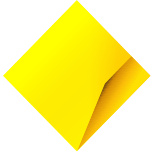
CBA believes there is merit in a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda. Cyber security is distinct from traditional STEM education in the sense it is multidisciplinary and, given it counters human adversaries, requires application of a specific mindset, understanding of attack tactics, human vulnerabilities, system complexities, and processes as well as technology.

The current approach to STEM has not yielded a cyber-ready workforce that is sufficient to satisfy demand. Data collected by the International Information System Security Certification Consortium (ISC)2 puts the current shortage at 25,000 professionals, while National Skills Commission (NSC) data indicates that we will need an additional 30,000 over the next four years to keep up with our rapidly changing security needs.[10]

Australian should approach cyber skills in the same way as it has digital literacy, with the development of a national cyber curriculum, which extends from primary, secondary, to tertiary education and can ensure a consistent and reinforced knowledge base. This curriculum could be introduced to schools as cross-curriculum priorities to show that cybersecurity is a consideration across a number of disciplines and industries and not as a stand-alone subject. This would lead to cyber proficiency whereby all school students have ongoing contact with cyber skills which supports an understanding that we need not only cyber specialists but also a modern workforce that has a baseline cyber capability. This is especially so in fields such as software engineering but equally applies in any field touching on data and money. We see the impact of this lack of baseline cyber knowledge frequently and believe curriculums at secondary and tertiary levels would help to address this.

Creating a cyber-focused approach not only will ensure consistency in knowledge but also see individuals who do specialise, reach industry accreditation earlier.

[10] Upskilling and expanding the Australian cyber security workforce, September 2022, page 9 https://cybercx.com.au/cyber-skills-report/



To complement the curriculum, a network, linking industry and educational providers should be formalised nationally. This initiative could be led by the ACSC, with a national network of institutions sharing cyber resources allowing the provision of real world industry input into teaching resources without needing to negotiate individual contracts each time an organisation wants to support an education institution on cyber course content.

To support development of Australia's cyber security workforce, CBA recommends:

- Taxation and immigration laws need to be reviewed to enhance the competitiveness of Australia's labour market and attract cyber skills. Currently, Australia risks losing cyber talent and suffers from periods of workforce disruption due to compliance obligations that restrict where cyber professionals can work and for how long.
- Organisations should be incentivised to offer entry-level roles that involve technical training for those with long term potential. Due to the labour shortages, skilled professionals tend to move between organisations rather than growing the workforce base. To this end, programs that offer cyber apprenticeships with funding available for employers to take on junior staff, or establish professionals seeking a career change, could be used to expand our cyber skills base, in the same way we do for other trades.

6. National frameworks to respond to major cyber incidents (questions 13-14)

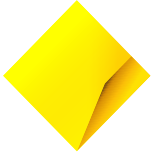
At the time of a major cyber incident, national frameworks, such as the Trusted Information Sharing Network (TISN), should operate to maximise collaborative and productive working relationships between industry and government. Optimising national frameworks accordingly would streamline information flows, allow for a more agile response to the cyber incident, and provide consumers with confidence that the collective industry and Government response is working in their best interests.

As noted above, the regulatory approach to incident reporting is illustrative of the problem of duplication and inconsistency. Duplicative obligations with triggers that do not align can have genuine operational consequences during a crisis and greatly affect an organisation's ability to respond. Crucially, it can draw front-line staff away from their core roles of responding to the incident, driving additional staff into incident response, increasing complexity.

As an example, depending on the cyber-incident, CBA may have to meet the following reporting obligations (in addition to responding to the attack):

- Immediately upon becoming aware of an incident CBA would be required to notify the Reserve Bank of Australia, and then every 30 minutes if the incident is New Payments Platform-related.
- Within 12 hours, CBA would be required to notify the ACSC under the Critical Infrastructure rules.
- Then, within 72 hours CBA would have to notify APRA.
- If the proposed ransom reporting obligations are introduced, CBA would also have to report to the ACSC within 21 days.
- 30 days to assess whether a data breach is an eligible data breach before notifying to the OAIC as soon as practicable.
- Report to ASIC within 30 days.

In addition to continuous disclosure obligations under ASX Listing Rules, there may also be reporting obligations to the SWIFT Payment Network, under the Payment Card Industry Data Security Standard,



and General Data Protection Regulations in the EU and UK. The latter requires reporting with 72 hours. Each incident reporting obligation comes with different forms and required information.

The single reporting portal should sit within a Government body that can support incident response. Other regulatory bodies that have a desire to be kept across a cyber-incident, though no role in supporting incident response, should be able to obtain the notification information from the reporting portal. Consideration should also be given to how this portal could be made available to any state government entities which may have a role in responding to a major cyber incident or managing consequences thereafter (e.g. reissuing driver licenses to address risk of ID theft).

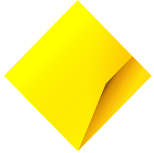
CBA notes this aligns with reform directive 14 offered by the Productivity Commission in its recent 5-year Productivity Inquiry which notes that a single reporting interface would reduce the administrative cost on businesses associated with the current plethora of reporting requirements to multiple regulators.[11] Proposal 28.1 of the AGD's Privacy Act Review Report, has also flagged "undertaking further work to better facilitate the reporting processes for notifiable data breaches to assist both the OAIC and entities with multiple reporting obligations."[12]

More broadly, Government can play a pivotal role beyond the current regulatory and operational framework in response to cyber incidents through:

- Helping coordinate and facilitate engagement and action in real time during attacks. This coordination and facilitation would be especially important during large-scale attacks where a number of critical infrastructure assets may be impacted.
- Better leveraging some of its existing communities and networks e.g. Trusted Information Security Network (TISN). As part of the Government's efforts to improve collaboration and information sharing as part of the TISN, the Government should consider promoting a form of standardisation in threat reporting schemas as a means for automating sharing and ingesting threat and intelligence data. Reporting frameworks, such as VERIS, use a common language and a structured, repeatable process, both of which allow organisations to classify security incidents.
- Utilising the offensive capabilities of Government to interrupt malicious threat actors. This capability would act as a deterrent to those targeting Australian organisations.
- Facilitating a proactive scheme for the sharing of breached data within a trusted network so that organisations can work to protect impacted individuals from harm. Pre-agreed information handling and security protocols are critical to success and operation at speed.
- Establishing a database or mechanism that sets out attack details such as the originating country, tactics, techniques and procedures as well as other key learning can be shared in real time with other critical infrastructure operators. If provided in a timely manner, this threat intelligence could help prevent organisations falling victim to similar attacks.
- Finalising the Trusted Digital Identity Framework which carries the potential to help protect the confidentiality of individual's identity documents and the impact an organisations data breach might have on them.

CBA would welcome development of a Government Post-Incident Review (PIR), as proposed in the discussion paper. Lessons drawn from the PIR should be disseminated to drive the development of cyber best practice and increase awareness of emerging cyber risks.

[11] https://www.pc.gov.au/inquiries/completed/productivity/report/productivity-recommendations-reform-directives.pdf
[12] https://www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf



CBA cautions that a consequence management model involving punitive measures may be detrimental to a post-incident review process noting that there may be reluctance from companies targeted by cybercrime, particularly small businesses who would be disproportionately impacted by a large financial penalty, to share details of a cyber-incident.

7. Victim and small business support (question 15)

Evidence from the ASD published in 2021 determined that while levels of concern about cybersecurity were high, with one in two Australians indicating their concern – only one in four considered themselves to have a good understanding of cyber issues and many are failing to take basic steps to boost their security.[13]

As outlined by the discussion paper, there is no consistent understanding of the practical steps that consumers, small and medium-sized enterprises (SMEs), and other organisations must take to enhance their cyber security. CBA believes there are opportunities to provide help the community build their understanding of where to report incidents of cybercrime and increase awareness of the practical steps they can take to stay safe online.

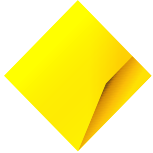
Consumers don't always distinguish between scams involving technology and cybercrime. Asking a victim to distinguish between the two as a first step to getting help can be a significant structural barrier and exacerbate the emotional, physical and financial harm caused. CBA encourages Government to provide a single reporting channel for victims to report crime associated with technology, including scams, and notes the development of the National Anti-Scam Centre within the ACCC which may provide such a role.

More generally, a streamlined, universal, and coordinated approach to proactive and protective cyber security messaging is required. Cybersecurity communication material should be designed for those who are most vulnerable to cybercrime and include clear, actionable steps consumers can take to protect themselves online. The current approach largely relies on digital channels such as websites and social media, which has limitations in reaching vulnerable community members, including older Australians and linguistically diverse communities.

Similarly, for small businesses, the strategy should raise awareness of cyber threats and build capability of the nation's small business workforce to identify and respond to cyber threats. Importantly, it is critical for the Government not to consider small business as a homogenous group in relation to cyber risk and vulnerabilities. For example, a small business that trades primarily out of a bricks and mortar premise will have a lower risk profile than a small accountancy, conveyancing, or legal practice that accumulates large amounts of sensitive customer data.

CBA has focused our support for small businesses to enhance their cyber security through educational content delivered through our existing online and face–to-face channels. For example, our business bank regularly invites CBA cyber professionals to professional development days for specific industries and other customer events to present on understanding cyber risk, identifying cyber weak points, and how to mitigate those weak points by using people, processes and technologies. Through these events, we are able to amplify ACSC messaging.

[13] https://www.abc.net.au/news/2021-01-11/australians-turning-point-on-cyber-security-cyberattacks-crime/13018884



More recently, CBA announced a partnership with the Council of Small Business of Australia (COSBOA) and Telstra on the *Cyber Wardens* program. The program aims to empower small businesses to upskill their workforces and give owners and employees the tools they need to stay safe online, through a free and easy to use accredited e-learning platform.

In our experience, while many small businesses have a strong appetite to understand their own cybersecurity posture, many do not have the capability or bandwidth to adequately deal with the information security requirements for their business. To support small business, CBA would like to see a focus on ensuring that the Software-as-a-Service (SaaS) platforms ubiquitously used in small businesses are incentivised to build secure data management into their products, such as allowing businesses to specify how long they wish to retain data for. Ensuring vendors selling operational technology products into small businesses meet a reasonable standard of cyber controls would help small businesses operate more securely without adding to their already significant workloads.

8. Enhancing the Australian cyber security ecosystem (questions 16)

CBA considers prioritising the accelerated adoption of Digital ID across the economy as a key action towards enhancing the nation's cyber security ecosystem.

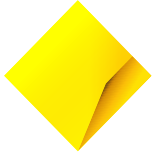
The Digital Identity system aims to improve convenience, as individuals no longer need multiple logins to access different services, and security, as identity verification is centralised to core identity providers (such as MyGovID or a bank) who invest more in protecting sensitive customer data. This means businesses across the economy do not need to collect and store sensitive information such as driver's licence and passport numbers in order to verify an identity, but can request the minimum customer data needed for their business purpose from an Identity Provider. Frameworks such as the Trusted Digital Identity Framework or ConnectID by Australian Payments Plus are designed to preserve privacy using rules and standards with individuals sharing only relevant details and service providers unable to seek further personal information without consent.

Fewer reproductions of sensitive information reduce the risk of third-party losses of personal information through security breaches. In practice, businesses can trust the Digital ID verification process conducted by a provider, accredited by the Government or other reputable schemes such as ConnectID, and avoid collecting a range of other data needed only to do the identity matching (such as document identifiers). This provides benefits to consumers by keeping their personal information safe and enhances the productivity of businesses by avoiding manual processes.

Digital ID also increases standards for data protection and transmission by requiring users to be compliant with best practice standards, such as having financial-grade APIs, in order to participate. Digital ID frameworks also promote business verifying customers against economy wide standards as opposed to using fragmented and industry wide-standards.

CBA urges the Government to take the following actions to accelerate the adoption of Digital ID across the economy:

- passing of legislation to enable the expansion of the Trusted Digital Identity Framework to the private sector;



- aligning anti-money laundering and counter-terrorism financing requirements to emerging Digital ID standards, and
- enabling the expansion of the Government's Facial Verification Service to the private sector.

Increasing the number of uses for the Digital Identity will also create 'network effects' whereby more organisations accepting a digital identity will encourage more users to sign up, which will in turn encourage more investment by organisations to accept that form of digital identity.

CBA supports recent recommendations by the Productivity Commission that the Australian Government work with the Council on Federal Financial Relations to increase access to its Digital Identity.[14]

9. Measurement and evaluation (questions 20 - 21)

Cyber resilience should be measured by the ability of Australians and Australian companies to respond to and recover from cyber-attacks.

As previously discussed, CBA would welcome the measurement of how many cyber simulations are held at a sector and cross-sectoral basis to ensure those organisations' cyber readiness addresses evolving cyber risks and that government systems are fit-for-purpose. Such exercises are essential to the evaluation of cyber security strategies and development of industry best practice.

In terms of how the Australian Government's cyber strategy is evaluated, CBA would first welcome additional consultation on the key mechanisms raised in this submission as a means to improving our cyber resilience, such as the single cyber regulatory and reporting body, development of a single Cyber Security Act, ASD/ACSC explicit obligation of confidentiality, and post-incident review.

To assist the Government in guiding the evolution of the Strategy overtime, CBA would welcome the permanent establishment of an advisory committee to provide advice to the Minister, much like how the Expert Advisory Panel has guided the work of the Strategy to-date. For example, in the US, the Cybersecurity and Infrastructure Security Agency (CISA), comprising leaders from across critical infrastructure sectors, provides advice on the development, refinement, and implementation of recommendations pertaining to the CISA's cybersecurity mission.[15]

[14] https://www.pc.gov.au/inquiries/completed/productivity/report/productivity-volume4-data-digital-dividend.pdf
[15] https://www.cisa.gov/resources-tools/groups/cisa-cybersecurity-advisory-committee