Cisco Systems Australia Pty Ltd

Level 14, 101 Collins Street
Melbourne Victoria Australia 3000

CISCO SUBMISSION TO AUSTRALIA'S 2023 CYBER SECURITY STRATEGY DISCUSSION PAPER

Cisco welcomes the opportunity to provide a submission to Australia's 2023 Cyber Security Strategy Discussion Paper and congratulates the Australian government and the Expert Advisory Board for the continued focus on ensuring the currency of this vital strategy.

As noted in our 2020 submission to the Australian Cyber Security Policy review, a cyber-enabled country is critical for a healthy, growing economy. Australian businesses and organisations that are not properly protected from cyber-attacks will negatively impact economic and jobs growth and constrain the policy choices available to governments.

This is especially the case as countries continue to accelerate their digital readiness and as organizations and businesses have overwhelmingly shifted their operating model from static – where people operated from single devices from one location, connecting to a static network – to a hybrid world in which they operate from multiple devices in multiple locations, connect to multiple networks, access applications in the cloud and on the go, and generate enormous amount of data. This presents new and unique cybersecurity challenges for companies and governments.

Australia is one of the most advanced digitally ready countries in the world according to the Cisco Digital Readiness Index which ranked Australia in the highest 'amplify' category. While this brings enormous opportunities for the Australian economy and community, it also comes with cyber security risks that must be effectively managed if Australia is to fully capture those opportunities.[1]

In March 2023, Cisco commissioned research to gauge organisations' own assessment of their readiness to meet modern security challenges and the results of the research were clear: no matter what kind of business you operate and no matter where you are, security resilience is imperative in today's hybrid world. The findings are documented in the *Cisco Cybersecurity Readiness Index: Resilience in a Hybrid World*[2]. The independent double-blind survey asked 6,700 cybersecurity leaders across 27 markets to indicate which solutions they had deployed, and the stage of deployment, across five key pillars - identity, devices, network, application workloads and data. Companies were then classified in four stages of increasing readiness: Beginner, Formative, Progressive and Mature.

- **Beginner (Overall score of less than 10):** At initial stages of deployment of solutions
- **Formative (Score of between 11 – 44):** Have some level of deployment, but performing below average on cybersecurity readiness
- **Progressive (Score of between 45 – 75):** Considerable level of deployment and performing above average on cybersecurity readiness

[1] Cisco Australia Digital Readiness Index 2022 https://www.cisco.com/c/dam/m/en_au/digital-readiness/pdfs/cisco-aus-dri-report-2022.pdf

[2]https://www.cisco.com/c/m/en_us/products/security/cybersecurity-reports/cybersecurity-readiness-index.html

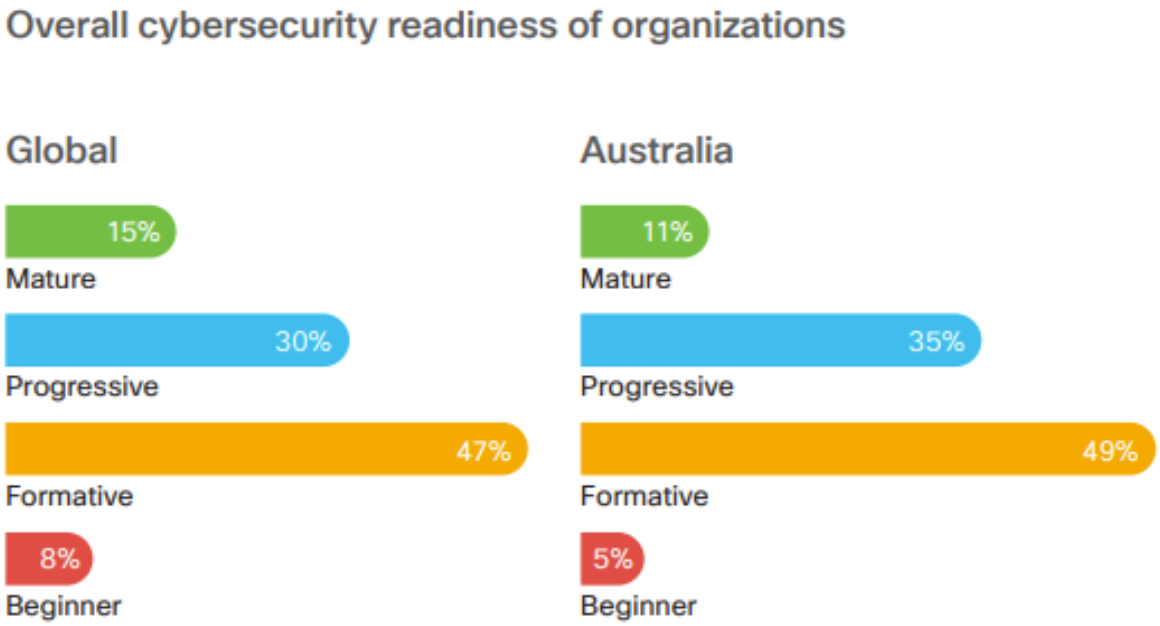
Cisco Systems Australia Pty Ltd

Level 14, 101 Collins Street
Melbourne Victoria Australia 3000

- **Mature (Score of 76 and higher):** Have achieved advanced stages of deployment and are most ready to address security risks

Alongside the stark finding that only 11% of companies in Australia are at the Mature stage, more than half (54%) of companies fall into the Beginner (5%) or Formative (49%) stages – meaning they are performing below average on cybersecurity readiness. Globally, 15% of companies are at a Mature stage – that is, they have a cybersecurity posture that is mature enough to defend against the threats of a hybrid world.

This readiness gap is telling, not least because 92% respondents said they expect a cybersecurity incident to disrupt their business in the next 12 to 24 months. The cost of being unprepared can be substantial as 70% of respondents said they had a cybersecurity incident in the last 12 months, and 69% of those affected said it cost them at least AUD $740,000.



This data suggests there is much work to be done if Australia is to reach the goal of being the most cyber secure nation by 2030 and this 2023 Cyber Security Strategy Discussion Paper is a key opportunity to identify areas of focus.

Please find below our responses to the questions in the Discussion Paper. Cisco welcomes the opportunity to provide further information, support and input as the policy development process continues.

1. *What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?*

Cisco Systems Australia Pty Ltd

Level 14, 101 Collins Street
Melbourne Victoria Australia 3000

Making Australia the most cyber secure nation by 2030 is an exemplary goal that will stand Australia in great stead if committed to, properly funded and effectively and efficiently implemented. Cisco has previously suggested the government set ambitious digital economy targets and commends the Minister and government for publicly committing to this goal.

Given the cost of cybercrime to Australia, this goal is required now more than ever.

The range of programs, education and technologies needed to achieve the goal will require significant investment from the Australian government, businesses and organisations. Australia has work to do to reach the same level that our global partners have reached in implementing an effective cyber strategy. For example, Australia will need to develop programs similar to those that the United Kingdom's NCSC Cyber Strategy[3] already has in place. Reports such as the National Cyber Security Index[4] ranks Australia at 40th, and highlights the following as the biggest gap areas:

- Protection of digital services
- Protection of essential services
- E-Identification and Trust services

There is a continued need to focus on protective mechanisms for scams, given that over two thirds of people are exposed to scams[5]. One idea for combatting scams would be for government to provide an easy way to report scams across multiple vectors (e.g., phone, SMS, email), automatic scam protections, and restricted number sending for key services.

Users are being targeted as an entry point into other businesses and organisations and this represent a significant risk. With 90% of business in Australia being small or medium businesses, the shift towards remote work, and growing attack surfaces in people's homes through network connected devices, it is crucial that the strategy focus on helping end users to be secure by default.

Areas that have been overlooked to date include ensuring access points or mechanisms have the right security capabilities built in, and that opt-out security services are offered to all Australians. Primary access mechanisms to the Internet for most users and small business are often through low-cost devices with controls that are left to be configured by end users who may be unaware or unable to protect their family, businesses and homes. To help manage this risk, the strategy could focus on adoption of protective mechanisms such as MUD RFC 8520[6] used with automated segmentation policy, as well as protection at scale with measures such as a Protective Domain Name System (pDNS).

The benefits of both building in more security into devices and leveraging tools like MUD enables more effective management of risk via automation at the network level. Ideally, MUD helps enable intelligent, intuitive networks understand the built-in capabilities and limitations of devices. However,

[3] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf
[4] https://ncsi.ega.ee/country/au/
[5] https://www.abs.gov.au/media-centre/media-releases/132-million-australians-exposed-scams
[6] https://www.rfc-editor.org/rfc/rfc8520

this functionality only works effectively and efficiently when the device is part of a system or network Even devices with security by design and by default—even those that are scrupulously maintained, patched, and configured—are going to eventually have their defences outstripped by the development of modern technologies and through the adaptations of threat actors. The network should be enabled to fill those gaps which is even more important given that we already have billions of devices online that were not built with security by design principles in mind.

So called 'clean pipes' initiatives should be part of the policy options available to government and the strategy is a good opportunity for government to have a public conversation about the benefits and disadvantages of deploying these technologies. Telecommunications carriers have done a good job of using automated technologies to block scam SMS and emails, so this type of technology is already in use and the public is benefitting from it by being exposed to fewer scams.

The strategy should also adopt principles and risk-based approaches for cyber security regulations. These are sustainable and flexible and avoid the pitfalls that specificity brings, as regulations quickly becomes obsolete as technology changes. However, there is disparity in how these approaches are received. There is a need for greater guidance as well as education, or cyber skills for business leaders and board members, to be able to interpret what is needed to meet risk-based cyber security regulations.

"Risk management" approaches have proven difficult for organisations to navigate and adds significant overhead, requires better guidance and more specificity around risk interpretation and guidance.

An important question to ask when re-evaluating the strategy is what should we do less of? Understanding what has been effective, and more saliently, what has not been effective, can better inform the strategy. The law of unintended consequences can affect the most well-meaning initiative. To this end, reviewing guidance and regulation is necessary. Are we making it easier for Australia to adopt a better cyber posture or more difficult? A focus on overall cyber outcomes would assist in understanding effectiveness of measures.

Australia is at the vanguard of internet regulation on cyber security and privacy. This is admirable and when regulation is undertaken in an orderly and consultative manner, the outcomes are usually optimal. However, Australia has also moved toward adoption of bespoke or localised certifications that can have unintended consequences such as creating a more complicated technology buying and vetting process, reduction in the choices of vendors and services that are available to the Australian marketplace and potentially higher costs for Australian businesses. The strategy should ensure that sovereign regulatory or compliance requirements do not exclude equivalent global certification requirements. In this way, the strategy will make security technology adoption simpler.

The strategy could also include Point-in-time checks and validations such as Common Criteria. Not only is the industry moving to faster, iterative development that renders point-in-time checks out of date faster, while the certification process remains lengthy. This makes the consumption of newer

technologies required to deal with a rapidly changing threat landscape more difficult and subject to longer delays. The UK NCSC has taken a more nuanced approach[7] with this understanding, and it is an opportunity for Australia to follow suit.

Concepts such as localised data and service sovereignty have arisen in numerous jurisdictions. For the utmost critical data and services, this can be a valid approach; however, this represents a very small subset of services. The rationale behind this growing trend is counter to the fact that many of the underpinning functions of the Internet are based around global cooperation (such as DNS, routing). Localization requirements need to be carefully considered to ensure it is not adding unnecessary time and cost to business nor closing off Australia to advanced cyber security and other technologies.

The simplification of governing bodies around cyber remains an opportunity in Australia. Many government organisations and agencies have different approaches from each other. Streamlining cyber accountability would aid the faster implementation of a cohesive cyber strategy and the recent announcements on the creation of new positions in the Department of Home Affairs are a step in the right direction.

In the case of E-Identification and trust services, emerging Web3 based identity technologies are ways of both maintaining resiliency and independence of identity services, while decoupling them from credential issuance process. Such approaches solve some of the digital identity and privacy problems we face but will require a strong government and industry partnership to achieve.

2. *What legislative or regulatory reforms should Government pursue to: enhance cyber resilience across the digital economy?*

Separate to the question of regulatory reform, which is discussed in following question responses, it is important to also investigate incentives for organisations to voluntarily achieve these outcomes through mechanisms such as tax and depreciation incentives. Cisco has previously suggested that specific financial incentives targeting SMBs through grants would be more effective than tax write-offs or depreciation due to cash flow challenges. An example is the current $220m government funding for technology adoption under the Strengthening Medicare policies, where GPs can seek grants for new technologies that improve their ability to deliver Medicare funded services to citizens and accommodate new technologies that could assist in better community health care.[8]

   a. *What is the appropriate mechanism for reforms to improve mandatory operational cyber security standards across the economy (e.g. legislation, regulation, or further regulatory guidance)?*

[7] https://www.ncsc.gov.uk/information/common-criteria-0
[8] Strengthening Medicare General Practice Grants Program Strengthening Medicare – General Practice Grants Program | Australian Government Department of Health and Aged Care

The approach used in the Security of Critical Infrastructure (SOCI) amendments of mandating action but at a principles and obligations level allows organisations to choose standards and frameworks that are both relevant to and right sized to their business. Mandating operational cyber security principles which are supported by implementation guidance, education, and assistance would be more beneficial than an approach of, for example, mandating a level of Essential 8 maturity that does not necessarily treat the priority threats faced by organisations of different scale and maturity. The Essential 8 is valuable guidance that organisation can adopt if appropriate in meeting a principles-based approach.

b. Is further reform to the Security of Critical Infrastructure Act required? Should this extend beyond the existing definitions of 'critical assets' so that customer data and 'systems' are included in this definition?

The recent amendments to the SOCI Act following the finalisation of a longer period of consultation with industry, academia, and the wider community are welcomed. The basis of input from industry was that the Act was securing '*those physical facilities, supply chains, information technologies and communication networks, which if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic wellbeing of the nation, or affect Australia's ability to conduct national defence and ensure national security.'* – a definition taken from the Critical Infrastructure Resilience Strategy Plan (2015) and (2023). This informed much of the conversation of the definition of assets in each sector and the thresholds and other criteria for determining what is a critical asset. The SOCI Act already contains an asset definition of "The meaning of an asset includes a system, network, facility, computer, computer device, computer program, data, premises and "any other thing." Within the Data Storage and Processing Sector, one of the criteria for criticality is 20,000 or more personal records.

While the SOCI personal records criteria is specific to one sector and hence does not capture all such datasets in Australia and the similar "systems" definition is only applicable to those within the 11 critical infrastructure sectors, we suggest that the further expansion of sectors or asset definitions under the SOCI Act is **not** desirable. The existing critical assets definitions were designed to capture only the most critical assets owned by an organisation – not all assets. Simply put, if everything is critical, nothing is critical.

Recent personal and sensitive data breaches in the telecommunications, health, and financial sectors, while "critical" to the individuals impacted who have suffered from the exposure of their personal information, they are not necessarily incidents that would likely impact the entire country or economy in the context of SOCI. An alternate means to assure appropriate protection of such personal data is through the Australian Privacy Act which also provides a greater ability to apply obligations extraterritorially whereas the SOCI Act only applies to assets held within Australia. Australia citizens' personal data requires protection irrespective of geography like Europe's GDPR arrangement.

Cisco Systems Australia Pty Ltd

Level 14, 101 Collins Street
Melbourne Victoria Australia 3000

c. Should the obligations of company directors specifically address cyber security risks and consequences?

The director obligations under the Corporations Act could be made more specific like the director obligations under *APRA Prudential Standards CPS 234: Information Security*[9] or through any future Cyber Security Act that defines Australian Cyber Security Principles. A specific reference to cyber security risks and consequences and obligations not only for company shareholder awareness but also other stakeholders and customers of a company would improve visibility and appreciation of the importance of good cyber hygiene and appropriate investment and funding.

d. Should Australia consider a Cyber Security Act, and what should this include?

The development of a new Cyber Security Act needs to consider the many existing laws and regulations that already exist in Australia. The Australasian Legal Information Institute (AustLII); University of Melbourne, Centre for AI and Digital Ethics; UNSW Sydney, The Allens Hub for Technology, Law and Innovation; and the Defence Science Institute have created a Cyber Law Mapping Project[10] that captures many of these. There is duplication and complexity depending on the type of asset needing cyber protection. A new Cyber Security Act needs to rationalise many other existing laws – potentially replacing them. A second consideration is to ensure a new Act is applicable to all and importantly implementable by all. From a sole trader through to large enterprise, there is a wide range of cyber security capability and affordability of measures that also needs to consider the relative value of assets being protected.

Rather than a new Act being overly prescriptive, which also introduces the risk of being coupled to the technology landscape of today, an alternative approach would be to define a set of Australian Cyber Security Principles (ACSPs) like the Australian Privacy Principles (APPs). Allowing applicable ACSPs to be implemented as obligations to relevant organisations under a reformed Privacy Act or any other Act would allow the principles to be chosen or developed "fit for purpose" to the appropriate cyber security guidance or frameworks, many of which are already in place though sometimes voluntarily today. An Australian small business may implement or work with a provider to achieve Essential 8 Maturity Level 1 whereas a large enterprise might implement AS/ISO27001 – a direct example of the flexibility in the SOCI risk management program rules for Cyber Security hazards.

[9] https://www.apra.gov.au/sites/default/files/cpg_234_information_security_june_2019_0.pdf
[10] Cyber Law | CyberLaw | AustLII Communities

Cisco Systems Australia Pty Ltd

Level 14, 101 Collins Street
Melbourne Victoria Australia 3000

e. How should Government seek to monitor the regulatory burden on businesses as a result of legal obligations to cyber security, and are there opportunities to streamline existing regulatory frameworks?

It is important to recognise where legal obligations, and methods to meet them, are already in place and avoid duplication. Recognition of adequacy of existing arrangements and frameworks, both domestically and internationally, is beneficial to industry. The SOCI Risk Management Plan Rules[11] are an excellent example of adequacy recognition in both the cybersecurity and personnel security hazards. They have reduced the Risk Management Plan (RMP) cost impact for some organisations.

Metrics are needed to measure success and provide transparency of any cyber security strategy initiatives as posed in questions 20 and 21 of this Discussion Paper. Such metrics are important to understand the effectiveness of measures towards a desired outcome. These could also be used to identify areas to streamline existing regulatory frameworks. For example, where a security outcome is being achieved under one initiative or regulatory framework, there is the ability to streamline through rationalisation and de-duplication of other regulations that are no longer required.

Regulatory Impact Statements are an effective way to measure the cost of regulation on the economy and the process undertaken for the SOCI legislation was exemplary. However, given the breadth of regulation associated with cyber security and privacy compliance, government should consider the cumulative cost of regulation on businesses and organisations.

f. Should the Government prohibit the payment of ransoms and extortion demands by cyber criminals by: (a) victims of cybercrime; and/or (b) insurers? If so, under what circumstances?

We are supportive of current guidance in the Australian Ransomware Action Plan where payments are not condoned but still permitted. They should be allowed, but considered as a means of last resort, specifically for data encryption ransom. Preference should be given to other methods of system recovery, such as restoring from backup. Importantly, paying a ransom does not guarantee data integrity once recovered. The cyber criminal may have deliberately modified data prior to encryption or there could be some corruption through the decryption process. Ultimately, a recovery from trusted backups or rebuilding of systems from a known trusted source may be required to regain trust in the integrity of data and systems. Payment of a ransom (for decryption) does not address these concerns.

For "double extortion" or data exfiltration ransom incidents, any payment should not relieve the organisation from any obligations or reporting – both to regulators and customers. For a purely data exfiltration ransom, we do not believe it should be considered a means of last resort to restore

[11] https://www.homeaffairs.gov.au/reports-and-pubs/files/soci-rmp-rules-legislative-instrument-lin-22-018.PDF

Cisco Systems Australia Pty Ltd

Level 14, 101 Collins Street
Melbourne Victoria Australia 3000

business operations, but at best, a harm minimisation measure *if* the attacker can be trusted. Similar to encryption related ransom, the organisation impacted must still attest to data integrity, remediate the attack vector, ensure there is no persistence or other action. A ransomware payment for exfiltration does not necessarily represent any cost avoidance.

The topic of banning ransomware payments has been long discussed[12] and should not be made in isolation of the full response options in the international and local ransomware action plans.

i. What impact would a strict prohibition of payment of ransoms and extortion demands by cyber criminals have on victims of cybercrime, companies and insurers?

For companies who find themselves with no means of recovery from backups, a strict prohibition of ransomware payments may impact the ongoing viability of the company itself. This is a type of scenario where a payment as a means of last resort should be considered.

In some critical infrastructure industries where the organisations' primary obligation is to get the service restored as soon as possible, prohibiting the payment of ransom could conflict with their ability to meet their obligations. That said, the Australian government may reasonably conclude that payment of ransom should be a trigger for mandatory notification to an appropriate law enforcement agency. Mandatory notification of payment notifications would also allow law enforcement to potentially disrupt or recover payments elsewhere in the ransom process or identify the recipients of the payment. The timely awareness of a proposed or actual payment would assist law enforcement in this case.

g. Should Government clarify its position with respect to payment or non-payment of ransoms by companies, and the circumstances in which this may constitute a breach of Australian law?

Clarification of laws which may be breached by a ransomware payment both under Australian law and other countries where Australian businesses may operate (such as the United States Treasury Department's Office of Foreign Assets Controls) would be beneficial and an area of international consensus the International Counter Ransomware Task Force could investigate. As mentioned previously, the payment or non-payment of a ransom is just one element of a comprehensive approach proposed by the Institute for Security and Technology Ransomware Task Force, the Australian Ransomware Action Plan, and International Counter Ransomware Initiative of which Australia is participating and chairing. Any prohibition of ransomware payment cannot be made in isolation of the other elements of these approaches.

[12] https://blog.talosintelligence.com/ransomware-extortion-roundtable-government-payments/

Cisco Systems Australia Pty Ltd

Level 14, 101 Collins Street
Melbourne Victoria Australia 3000

3. *How can Australia, working with our neighbours, build our regional cyber resilience and better respond to cyber incidents?*

We recognise and support the government's existing efforts through Australia Cyber and Critical Tech Cooperation Program. Various industry initiative and partnerships delivered in Australia are also delivered to our regional neighbours such as the Cisco Networking Academy. The program is being expanded to the Pacific Islands to help those countries address the cyber and STEM skills gaps. Opportunities to replicate other public-private partnerships already delivered in Australia could be explored.

4. *What opportunities exist for Australia to elevate its existing international bilateral and multilateral partnerships from a cyber security perspective?*

Recognising the adequacy of other country cybersecurity polices and implementations combined with recognition of equivalency in legislative frameworks regarding safeguards from government overreach could set the basis on trust for areas such as data hosting (cloud) or addressing supply chain risks. This would not only ensure Australian organisations (and government) have access to a wider range of services and improved resiliency through greater geographic area diversity, but also offer the same opportunities for Australian organisations to expand into partner countries with reduced infrastructure investment costs.

This is particularly true where our defence arrangements are highly interdependent on other countries (such as the "Five Eyes" nations), but we are unable to leverage the same countries for sensitive data processing in some cases.

5. *How should Australia better contribute to international standards-setting processes in relation to cyber security, and shape laws, norms and standards that uphold responsible state behaviour in cyber space?*

Organisations such as Standards Australia and other government departments and agencies should actively participate in standards setting and guidance creation, not only in international standards bodies but also in partnering with peer nations, such that the outputs are recognised as valid standards in Australia and certifications against those standards recognised without additional local testing. This is the case with AS ISO/IEC 27001:2015 and internationally updated to ISO/IEC 27001:2022, which are used by enterprises and governments around the world as a tool for cyber risk management. Given the interconnected nature of our networked environments globally, it is also increasingly important that the same international standards are used for vulnerability handling (ISO/IEC 30111:2019) and disclosure (ISO/IEC 29147:2018).

Cisco Systems Australia Pty Ltd

Level 14, 101 Collins Street
Melbourne Victoria Australia 3000

6. *How can Commonwealth Government departments and agencies better demonstrate and deliver cyber security best practice and serve as a model for other entities?*

We have previously called for agencies to act as exemplars of data stewardship. A leader in cybersecurity needs to go further than this. There is a need to adopt best practices for digitisation with a focus on security and resiliency and protecting citizens. Clear and protected communication channels for all key governmental services will create difficulties for scammers to imitate and spoof.

7. *What can government do to improve information sharing with industry on cyber threats?*

The government, through the Australia Cyber Security Centre (ACSC), has implemented various information sharing programs with industry including the ACSC Partnership Program, Joint Cyber Security Centres, Cyber Threat Intelligence Sharing (CTIS) and the CISC TISN expansion. Opportunities to improve information sharing need to start with a review of the success, value, and where identified gaps not addressed by these existing programs. Key aspects to maintain focus on are: ensuring information shared is actionable at the lowest level of classification possible and information is timely both in the creation but also automated means of delivery and consumption.

8. *During a cyber incident, would an explicit obligation of confidentiality upon the Australian Signals Directorate (ASD) Australian Cyber Security Centre (ACSC) improve engagement with organisations that experience a cyber incident so as to allow information to be shared between the organisation and ASD/ACSC without the concern that this will be shared with regulators?*

Yes. A formalised safe harbour provision for ACSC engagement to allow timely and valuable assistance to be sought from the ACSC at the operational incident response level could provide organisations the confidence that reporting confidentiality obligations to regulators can be managed in the required timeframes and appropriate channels.

Contradictory objectives for companies to both comply with timely incident engagement with the ACSC on incidents and have penalties imposed for having incidents may cause pause or require legal gates to be in place. Cisco actively encourages rapid and open threat intel sharing through automated fashion, allowing all parties better situation awareness and actionable threat intelligence.

Threat intelligence alone does not allow rapid response to limit damage in data loss circumstances with third parties (e.g., privacy or sensitive data). Engagement with the Australian Signals Directorate (ASD) could help with response activities to limit impact. As such, any activities that permit earlier engagement with bi-directional trust with ASD and relevant parties should be encouraged.

Cisco Systems Australia Pty Ltd

Level 14, 101 Collins Street
Melbourne Victoria Australia 3000

9. *Would expanding the existing regime for notification of cyber security incidents (e.g. to require mandatory reporting of ransomware or extortion demands) improve the public understanding of the nature and scale of ransomware and extortion as a cybercrime type?*

It is important to recognise the different types of incidents and the differing notification requirements that might then apply. Incident notification requirements for a threat and security incident requires timeframes to assess significance and whether minimum reporting thresholds have been met else regulators and organisations alike will be overwhelmed but the volume of low-level security events that are experienced daily. Similar consideration needs to be given to the reporting of ransomware demands and ransomware payments. However, a ransomware payment is a discrete event and mandatory reporting of a payment regardless of the scope of an incident or severity should be considered for the reasons mentioned earlier.

It is not clear what outcome is being sought by increasing public awareness of ransomware and extortion. Potentially, it may drive action by organisations to improve security or risk reputational damage and/or reduce public harm. But, noting the public are often also employees or business owners, there is also a benefit of improving the general awareness and security culture of the Australian population at large, so to that end we support greater awareness. As such, measuring that goal against the existing notification obligations under the Privacy Act (including outcomes from the ongoing review) is needed before any further expansion of the notification regimes. While the question is posed specific to ransomware and extortion, any expansion of notification schemes could cover other types of incidents such as business email compromise to also improve public understanding – noting that the public are often employees so personal awareness benefits business and vice versa.

10. *What best practice models are available for automated threat-blocking at scale?*

Through previous cyber strategies and industry initiatives, many examples of automated threat-blocking already exist – coverage and uptake should be the focus along with a continued focus on the efficacy and effectiveness of the solutions. For web threats, Protective DNS is a clear mechanism to provide such threat-blocking. Coverage by default can be limited to public sector users of AUpDNS, major Australian ISPs who provide it as part of their residential and business Internet services, and enterprises who chose to purchase and deploy such a solution. It is unlikely that a user driven demand model will increase coverage and hence a regulated “clean pipes” service approach might be required. Progress has been made by major Australian telecommunications companies in addressing SMS phishing and other threats at scale. Desktop and mobile device operating systems manufacturers and vendors have significantly addressed the window of exposure for vulnerabilities in the consumer space through auto update by default mechanisms – yet this does not extend to all connected devices in an Australian home today. An opportunity to extend cyber resilience in the home exists with the home CPE router as a control and visibility point. Similarly, major email service providers provide the base level of protection for email-based threats. However, there are many organisations that are not

covered by these protections or who require a higher level of protection against, for example, business email compromise.

We suggest a review of existing threat-blocking at scale solutions such as the above and the results they are delivering today. There are opportunities to expand coverage and recognise that they provide a baseline of protection, though not total protection, thus requiring other capabilities.

11. Does Australia require a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda?

The cyber skills discussion needs to move beyond "cyber roles," and towards whole of Australia cyber literacy. In addition to cybersecurity specific roles, legislators, boards, business directors, employees, and householder literacy are all just as important. In our organisation, security is everyone's responsibility. This requires us to help educate everyone. Often cybersecurity skills are seen as we need more defenders or protectors. What are the skills needed to avoid some of the problems in first place; privacy impact specialists – why collect the data in first place, data stewards? Why retain data? This is part of secure development and secure by design, designing systems to be defensible and updateable. If we want to "shift left" some of the cybersecurity responsibility, what jobs does this impact that then need appropriate cyber skilling.

Cisco had made significant investment in our Networking Academy (NetAcad) program to expand beyond networking to include areas such as cybersecurity, IoT, data science, and infrastructure automation. Globally, Cisco Networking Academy has supported over 17 million students since 1997. Our goal to not only expand the pool of available workers with requisite skills, but also to develop new pipelines of talent from non-traditional populations, which has the potential to help expand the diversity of the cyber-skilled workforce. Powered by our Networking Academy, the Cisco Skills For All is an example of the type of program to attract both a diversity of people to pursue STEM related employment or provide them STEM related skills in their current role. [13]

In 2014, Cisco launched a Country Impact Plan which had the ambitious goal of training 100,000 students in STEM skills through the Cisco Networking Academy program, a goal that we exceeded by some 20,000 students. Over 80% of Cisco Networking Academy students go on to either further study or take up employment. Recently, in the United States, Cisco committed to training 200,000 students over three years in cyber security skills along with pledges from other industry and education partners as part of a White House hosted National Workforce and Education Summit.[14]

The new cyber security strategy should include specific goals for training new cyber security workers and re-training those workers who wish to make a transition into the technology industries. Engaging

[13] https://skillsforall.com/

[14] FACT SHEET: National Cyber Workforce and Education Summit | The White House

Cisco Systems Australia Pty Ltd

Level 14, 101 Collins Street
Melbourne Victoria Australia 3000

with industry players who have created accredited job-ready education programs and who work in partnership with Australian schools, TAFEs and Universities to deliver these programs is essential.

Notwithstanding these efforts, we should also recognise the lack of available workers more generally and the increasing demand contributed to by technology development and digitisation. In parallel to skilling, we should then also look to greater automation to help address both the shortfall in workers but also scale capabilities to machine and network speed.

12. *What more can Government do to support Australia's cyber security workforce through education, immigration, and accreditation?*

Since the 2016 strategy, significant progress has been made in the availability of cybersecurity education both at university and vocational education and training levels. Incentives to support cross-training and a lifetime learning approach through micro credentialling could be explored to ensure the existing Australian workforce maintains relevant skills.

13. *How should the government respond to major cyber incidents (beyond existing law enforcement and operational responses) to protect Australians?*

One area of investigation is how to quickly share not only the threat intelligence but put in place protection for other organisations that not yet been impacted. Participation in CITIS or actioning ACSC advisories required a degree of organisational maturity. The government could investigate how to quickly share where appropriate and available threat intelligence and IOCs with security managed service providers (MSPs) and security industry vendors so protection can be quickly delivered to other Australian organisations via automatic rule updates, verdicts, etc., in the products they already have deployed.

a. *Should government consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators?*

From a streamlining of operational security viewpoint this makes sense, however this is complicated by different reporting timeframe obligations and different reporting content. Any single reporting portal should give the reporter control over which regulator have awareness of a report and visibility of the content of a report.

Consideration would need to be given on how to maintain the separation between the ACSC assistance and advice function and regulator reporting. Given the possibility of safe harbour provisions to work openly with the ACSC, a separate dedicated single portal for regulator operated by other than the

ACSC may be required rather than expand the existing ACSC incident reporting portal to other recipients.

Any single portal for reporting information should aim to support automation and making it easy for everyone to report issues via flexible channels – such as through API, email, and voice. Automation benefits the processing and consumption of the reports as well, assisting with dissemination of relevant information in timely manner.

14. *What would an effective post-incident review and consequence management model with industry involve?*

Post incident review, irrespective of the cause, is a great learning experience. Such reviews need to be blame free for greater effectiveness, with the aim to learn and respond. Safe harbour provisions discussed earlier should be considered.

15. *How can government and industry work to improve cyber security best practice knowledge and behaviours, and support victims of cybercrime?*

Specifically, to reduce harm to victims of identity theft cybercrime, there should be consideration on ways to reduce the amount of identity data held by organisations. For example, mobile providers can be allowed to rely on the Trusted Digital Identity Framework (TDIF). Options should be investigated to reduce the ability to monetise stolen identity data and reduce the value / usefulness of that data.

a. *What assistance do small businesses need from government to manage their cyber security risks to keep their data and their customers' data safe?*

Small business owners need to become more cyber aware. They need tools and process to not only secure their business but secure their customers data. A focus on business cyber skills would be appropriate. The government, through the ACSC and industry groups, has produced valuable awareness and education materials through platforms such as cyber.gov.au. It is not clear that metrics and measurements are in place to gauge the effectiveness of this assistance.

16. *What opportunities are available for government to enhance Australia's cyber security technologies ecosystem and support the uptake of cyber security services and technologies in Australia?*

Government can and should undertake a 'stocktake' of investments in the Australian eco-system to better coordinate and leverage the investments that industry are making in the Australian cyber security eco-system.

For example, Cisco has invested in the Australian Cyber Security CRC along with others to advance research and development capability in Australia. In addition, Cisco has invested in a National Industry Innovation Network (NIIN) which is an alliance between industry and universities driven by one goal: to realise digital opportunities that can benefit the lives of all Australians. The NIIN is working on nationally significant projects, including securing critical infrastructure, education, digital health and hybrid work through a range of initiatives including funding for research chairs; education and training partnerships with universities and TAFE's; establishing a network of innovation centres (Innovation Central) that undertake digital research projects that solve real-world problems brought to the centres by industry; and skills and talent development such as the Australian Cyber Collaboration Centre at Lot 14 in Adelaide. Cisco also invested in a Cyber Security training centre at the St Albans Campus of Victoria University in Melbourne that is training new students and re-training existing workers in cyber security skills. Many of these investments by industry are not fully leveraged when policy makers are considering solutions to skills shortages or looking to develop Australian eco-system capability.

Ensuring that Australia is able to access and leverage the best cyber security technologies and talent from around the world is vital to the growth and capacity building of the Australian cyber security eco-system.

17. How should we approach future proofing for cyber security technologies out to 2030?

Given the rapid pace of technology development, we suggest two initial approaches for policy to remain relevant and applicable. Firstly, aim to define the outcomes and intent of policy followed with principled based obligations decoupled from technology. Secondly, ensure the Australian Cybersecurity Strategy 2023 is reviewed annually and updated at least once in two years. Strategy releases in 2016, 2020, and now 2023 with a view to setting the direction to 2030, are not frequent enough to keep pace with technology developments and associated cybersecurity considerations. A wholesale re-write is not desired but rather maintenance as a "living (document) strategy" – areas can be revised, deleted if no longer required, or added as part of future proofing.

It is important to recognise that future technologies also bring opportunity - newer technologies can bring incrementally better integration, speed and capabilities as cyber security vendors innovate and evolve. Newer technologies should be encouraged.

Conversely, it is also important to recognise that avoidance of future technologies can contribute to technical debt or obsolescence. After many decades of IT adoption, the sheer number of vendors, and the large, heterogenous landscapes, most networks have outdated technologies, not just in security. In many cases, particularly across critical infrastructure, installation lifetimes far exceed vendor support lifetimes. Future proofing then also includes a systematic focus on cyber hygiene that

incorporates full lifecycle management of technology with deliberate proactive management of end of service / end of life milestones – rather than a "if it's not broken don't touch it" mentality. Planning for the future also requires bringing along technical debt from our past.

19. How should the Strategy evolve to address the cyber security of emerging technologies and promote security by design in new technologies?

Cisco would like to acknowledge ACSC as a joint author of *Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default*[15] *building on the earlier ACSC IoT Code of Practice Guidance for Manufacturers. This is valuable guidance which should be promoted widely. This guidance is targeted primarily at secure software development. There are areas of emerging technology where security by design would benefit from a more system level approach.*

There are two key areas of emerging tech that should be a focus: Quantum computing and cryptography, and AI and its threats, vulnerabilities and uses in cyber defence.

Security by design principles is a driver. There is a potential of adopting this approach across government and critical services, embedding cyber in all solution design. However, the shift towards continuous visibility, evaluation and risk measurement, as opposed to static point in time reviews and controls, is a more pressing need.

Quantum computing represents a challenge to existing encryption underpinnings of all digital services. The space is predicted to rapidly evolve, with continual iterations of quantum resistive algorithms being developed and evolved. The ability to build in the ability to deal with obsolescence of these measure in our services needs to be a consideration.

AI is another area that has received much attention of late. It represents potential rapid acceleration in many areas of cyber, and warrant a specific focus, both from investing in research, cyber tools, education and workforce planning.

18. How should government measure its impact in uplifting national cyber resilience?

We raised in our submission to the Australian Cyber Security Policy 2020 on how to determine whether the current cyber threat landscape in Australia is getting better or worse. Although this is phrased in 2023 as making Australia the most cyber secure nation in the world by 2023, the question is heavily dependent on what metrics are used and it also raises the question – are we measuring the right things?

[15] https://www.cisa.gov/resources-tools/resources/secure-by-design-and-default

Cisco Systems Australia Pty Ltd

Level 14, 101 Collins Street
Melbourne Victoria Australia 3000

The answer to the question of what metrics should be measured requires consultation and agreement between governments, industry and other stakeholders to establish and publish consistent benchmarking metrics about the threat environment. This will allow proper accountability of whether the cyber security policies and programs are improving the threat landscape.

If the measure is cyber resilience, then the metrics need to reflect the full spectrum of what is cyber resilience – at a high level to anticipate, withstand, recover, and evolve. At the cybersecurity operation level, for example, NIST's Cyber Security Framework with metrics can reflect progress or maturity across identify, protect, detect, respond, and recover.

This is a large topic but one that should have dedicated focus from government on an ongoing basis from the macros level; cybercrime revenue as a percentage of GDP through to specifics such as the window of exposure for unpatched known vulnerabilities through to trending such as changes in the root cause of malicious breaches reported to the OAIC (persistently dominated by credential related issues).

The previously mentioned Cisco Cybersecurity Readiness Index: Resilience in a Hybrid World research provides some specific guidance on metrics that could be included in a national cyber resilience uplift measurement exercise. [16]

19. What evaluation measures would support ongoing public transparency and input regarding the implementation of the Strategy?

As raised in our 2020 Cyber Security Strategy submission, any agreed metrics need to be reported annually. Australia's Cyber Security Strategy First Annual Update 2017 reported on "activity" against the 2016 initiatives. This was appropriate as many recommendations were related to the formation of and investment in new initiatives. Now that many of those are in place, Australia needs metrics on outcomes. Government, industry, and citizens need to know whether we are improving the cyber security posture of Australia and making progress against malicious actors. Regular (at least annually) progress reporting or even a continuous dashboard view of key measures should be considered.

Benchmark data will also inform the speed with which policies and programs are implemented and the scope and reach of interventions.

ENDS.

[16] https://www.cisco.com/c/m/en_us/products/security/cybersecurity-reports/cybersecurity-readiness-index.html