Cisco Systems Australia Pty Ltd

Level 14, 101 Collins Street

Melbourne Victoria Australia 3000

CISCO SUBMISSION TO AUSTRALIA'S 2020 CYBER SECURITY STRATEGY

Cisco welcomes the opportunity to provide a submission to the *Australia's 2020 Cyber Security Strategy: a call for views* and congratulates the Australian government for undertaking this vital policy renewal process.

A cyber-enabled country is critical for a healthy, growing economy. Importantly, failing to properly protect Australian businesses and organisations from cyber-attack creates a drag on GDP and jobs growth and is an economic dampener.

The government's development of a cyber security strategy in 2020 and implementation of that strategy is an opportunity for Australia to continue strong economic growth and creation of the jobs of the future.

Please find below our responses to the discussion paper and additional supporting detail through the attached documents.

Cisco welcomes the opportunity to provide further information, support and input as the policy development process continues.

Cisco's view of the threat environment

The threat environment since the release of the 2016 Australian Cyber Security policy has evolved. Attacks are more sophisticated, with low level, persistent attacks on IT and OT becoming more common and moving into the cyber physical space by attacking critical infrastructure. Cyber criminals continue to attempt to profit, cause chaos and steal data, despite improvements in median time to detect and contain by businesses, governments and organisations that have been improving their cyber security posture, defences and remediation capability.

It is useful to examine previous successful cyber threats and attacks as a guide for what we could expect in the future. When a cyber criminal discovers a successful attacking methodology, they will use it again and again as they continue to probe for gaps and weaknesses. Without closing these known vulnerabilities, individuals and business become the 'low hanging fruit' and easy targets. Quite often these systems become pivot points to attack the rest of the business.

Cisco Systems Australia Pty Ltd

Level 14, 101 Collins Street

Melbourne Victoria Australia 3000

In the *Cisco February 2019 Threat Report*, Cisco identified intricate and revealing details on five cyber threats, chosen not just because they were big events but because these threats, or something similar, could very well appear again soon. These threats are:

- Emotet, a trojan involved in malware distribution
- VPNFilter, a modular IoT threat
- Unauthorised Mobile Device Management
- Cryptomining, and
- Olympic Destroyer, an example of destructive cyberattack campaigns.

These five threats are important for the attack *trends* they represent. For example, modular threats download plugins or other threats, depending on either the type of device infected or the intended goals of the attackers:

- VPN Filter's third stage was dedicated to pulling down plug-ins to help the attackers achieve their intended goal
- Emotet's distribution system allowed for multiple payloads, from infostealers to ransomware, depending on the type of system it infected, and
- The successful installation of unauthorized mobile device management (MDM) profiles opens the door for an attacker to install any sort of malicious app he or she wishes.

Modular threats are therefore likely to continue to be used.

The threat environment has also seen a pivot to attacking the user since the 2016 Cyber Security Strategy. This could be attributed to the huge uplift in the market value of a zero days attack on a device, precisely because industry has done the right thing and made it more difficult to achieve. As industry has improved its secure development capabilities, attackers are now more likely to focus on the user because they are easier (and cheaper) to target through phishing and social engineering; they are the weakest link. This is particularly the case when it comes to cyber fraud, where users are targeted to authorise fraudulent payments.

The *Cisco 2019 Asia Pacific CISO Benchmark Study* surveyed over 2000 Chief Information Security professionals across the region. In Australia, the survey identified that:

Cisco Systems Australia Pty Ltd

Level 14, 101 Collins Street

Melbourne Victoria Australia 3000

- 84 per cent of organisations in Australia suffered a breach that cost them over $1 million, which is higher than any other country, in the APJC region and globally
- 69 per cent of Australian organisations reported receiving more than 100,000 alerts every single day, more than double last year's figure of 33 per cent
- 75 per cent of Australian organisations experienced an outage of 5 -16 hours. This is longer than the global average of 43 per cent
- Australian businesses are experiencing double the level of Cybersecurity Fatigue in comparison to the global average – Australia 65 per cent vs. global 30 per cent

A key issue for consideration in the Australian Cyber Security Policy 2020 will be determining whether the current cyber threat landscape in Australia is getting better or worse? This question is heavily dependent on what metrics are used and it also raises the question – are we measuring the right things?

The usefulness of non-Australian, volumetric data as metrics to gauge whether cyber security initiatives in Australia are making a positive impact is limited and the data is quickly outdated.

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.

For example, should the number of threats and attacks be reported as a percentage of digital businesses or online activity or cyber crime as a percentage of GDP and/or population? This will also assist in determining if government and industry and the community are slowing down cyber criminals, catching up or going backwards.

For a properly organised defense ecosystem, we need timely dissemination of threat intelligence. Measures of this may also encourage greater collaboration; was the attack a known threat? Are we organised to deliver industry specific threat intelligence in a timely manner?

These metrics then need to be reported annually. Australia's Cyber Security Strategy First Annual Update 2017 predominantly reported on "activity" against the 2016 initiatives. This was appropriate as many recommendations were related to the formation of and

Cisco Systems Australia Pty Ltd

Level 14, 101 Collins Street

Melbourne Victoria Australia 3000

investment in new initiatives. Now that many of those are in place, Australia needs metrics on outcomes. Government, industry, and citizen need to know whether we are "closing the gap" and improving the cyber security posture of Australia and making progress against malicious actors.

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

Key Recommendations:

- Adopt a wider range of metrics that measure progress against desired outcomes
- Stronger reporting requirements
- Yearly Annual Security Report

Building cyber into digital goods and services

As organisations and businesses become more digital, security must be more than a department or set of loosely-integrated solutions to keep up. It must be a total philosophy, worked into everything from product design to development and deployment and customer care, especially in the case of consumer goods and services.

This is especially important as the massive increase in devices that are connected to networks, with an estimated 14.6 billion IoT devices by 2022 according to the *Cisco 2020 Global Networking Trends Report*. Security should therefore be fundamental to the design of any device that will be network enabled, no matter where it sits in the economy.

As consumers become more aware of cyber threats through connected devices, incorporating secure design of digital goods and services into consumer warranties would provide a market advantage. This would put the emphasis on manufacturers to meet the standards they need to influence buyer behaviour in relation the cyber security.

Particular attention must be placed on defence in depth by adding security at all layers, not just at the device or through cloud services. No device can always be secured, so the network layer must be considered as an active protection (and detection) layer. Advances such as MUD (RFC 8520) are designed to assist with ease of managing this layer. Additionally, network layer devices should have similar requirements for security posture as endpoints.

Cisco Systems Australia Pty Ltd

Level 14, 101 Collins Street

Melbourne Victoria Australia 3000

End user internet services are one area that this becomes particularly relevant. Low end, unpatched consumer routers represent significant impact, particularly in healthcare with ever growing in-home treatment and critical medical devices connected in the home. VPNfilter was an example of an attack against these home routers, a trend expected to continue.

Changing consumer behaviour through education is critical to improving cyber threat protection. Consumer education campaigns that have been previously successfully could serve as examples. The star energy rating system for whitegoods and other home appliances provides a clear, easy to compare rating system on which consumers can make an informed choice. Today, consumers have no easy way of comparing products on factors like support lifetimes, SLA for security updates and security features such as secure boot, run time protection or secure storage capabilities.

While establishing a benchmark for a cyber security star rating would be complex and take some time, consumers, businesses and organisations could have the benefit of informed choice at the point of purchase. In addition, a clear and simple rating system would influence the market behaviour of manufacturers.

Finally, where standards or accreditations are established for cyber security in goods and services, appropriately resourced enforcement and compliance bodies are essential for system integrity and efficacy. There is little point in establishing a product standard or protocol that ought to be met if there are no penalties for not meeting it.

Key Recommendations:

- Security support as part of warranty
- Drive consumer home internet gateway minimum standards
- Consumer connected electronics labelling standard

The role of government in addressing the most serious threats to critical infrastructure, institutions and businesses located in Australia.

The return of cyber safety and security to the federal ministry is most welcome and reflects the importance that the government has placed on this policy issue. It ought continue to be a top national priority and have broad support across the Parliament.

Cisco Systems Australia Pty Ltd

Level 14, 101 Collins Street
Melbourne Victoria Australia 3000

Critical infrastructure

Cyber criminals and adversaries currently possess the expertise and tools necessary to infiltrate and attack critical infrastructure and systems. As an attack of that kind could impact entire regions and countries, there is clearly a need for government, industry, organisations and the community to work together to protect our critical infrastructure. Critical infrastructure protection improved significantly following the implementation of the 2016 Cyber Security Policy initiatives, through the ongoing maturing of industry standards, and the deployment of commercial off-the-shelf security technologies. However, in order to defend critical infrastructure from the cyber risks of today (and tomorrow), a holistic strategy is needed where security is embedded everywhere and integrated throughout the operations of every critical infrastructure provider across its people, processes and technology.

Critical infrastructure providers around the globe see technology as at the core of their operations and need to embed security everywhere, if they have not already. Whilst, there have been some Critical Infrastructure security incidents in Australia, we have not seen this to the level or impact of other nations and hence the challenge may be moving from awareness of the problem to action on the problem. Cisco agrees with the Australian Security Policy Institute's observation in their report "Protecting critical national infrastructure in an era of IT and OT convergence", that diverse ownership structures complicates addressing the gap between IT and OT security maturity. Any initiatives to tackle this program will likely need to be a blend of education, best practices, and regulatory and legislative enforcement in order to drive improvements across the multiple industry sectors.

Like any cybersecurity strategy, critical infrastructure providers need to take a risk-based approach to benchmark and understand where they are most vulnerable and identify how to address those risks. This requires a sophisticated capability to have visibility and control from the network as the trusted, critical risk control point. The network connects the data, programs, applications, web networks, software and hardware within a critical infrastructure provider's environment so it can deliver goods and services to end customers. Addressing this risk requires embedding security technology, processes and policies so the authenticity and integrity of each device can be verified as well as any hardware and/or software running on it.

Cisco Systems Australia Pty Ltd

Level 14, 101 Collins Street

Melbourne Victoria Australia 3000

Integrating security throughout the operations environment is essential to deliver the machine speed required to support better detection, visibility and control. This will have the added benefit of enabling solutions to work together, communicate and automate actions to make it easier to address incidents faster (machine speed) and less complex (does not rely on multiple human actions).

To secure critical infrastructure on a global scale will require more than just individual organisations, it is a multi-party responsibility including both the public and private sector. There is much to be gained through innovative partnerships that share best practices, collaborate on threat intelligence, teach how to build and deploy secure solutions, and bolster education and training. Whether it is joining industry initiatives like the Charter of Trust or actively working to combat cyber-crime in partnership with global law enforcement organisations like Interpol. Industry specific threat intelligence sharing also becomes a crucial practice.

Having government and other stakeholders involved in protecting critical infrastructure requires a high level of trust to be established. Australian citizens could rightly expect a high level of trust in the capabilities of government and other partners to protect critical infrastructure from cyber threats. This stems from a commitment to strong accountability and clear checks and balances that govern the regulatory regime and a commitment to open and transparent reporting of incidents. Informed citizens are more likely to have a higher level of trust and confidence.

In order to build that trust in Australia, considerations towards streamlining reporting and accountability across critical infrastructure should be considered. Operators should be held accountable to reporting on key areas of cybersecurity operations and preparedness. Reporting requirements combined with non-compliance penalties and liability for inaccurate or sub-standard posture, are the best way to influence cyber-resilience across organisations.

Key Recommendations:

- Simplify critical infrastructure reporting and regulatory ownership
- Implement strong penalties for non-compliance
- Measure the effectiveness of existing industry specific threat intelligence sharing for critical infrastructure such as the JCSC to identify opportunities to deliver further value

Cisco Systems Australia Pty Ltd

Level 14, 101 Collins Street

Melbourne Victoria Australia 3000

Institutions and businesses located in Australia

Enterprise sized businesses and organisations in Australia have made solid progress on better securing and protecting their operations from cyber security threats and attacks since the release of the 2016 Cyber Security Policy. While there is still much work to do, there is a growing awareness of the need for action and the allocation of resources to support improved an improved security posture.

Government has played an important role in this progress as outlined in Appendix A of the discussion paper and the ongoing investments being made to better coordinate and communicate cyber security threats.

An area worth additional focus is the small and medium business sector and Australian citizens.

Cisco congratulates the progress made by the ACSC in publishing the Small Business Cyber Security Guide. There is opportunity to build on this advice further to provide recommendations for improving the cyber posture of their network infrastructure such as their business routers, patching, segmentation, and credential hygiene for business IOT devices (security systems, multifunction printer, security cameras), and the need for a layered defence rather than a single protective mechanism. Recent incidents such as VPNFilter and the Mirai Botnet are examples of the need to expand SMB advice.

As part of layered defence approach, Government can play a role by ensuring that SMBs and citizens connected to the internet are aware of the benefits of quality DNS resolving services.

More than 91% of malware uses DNS to gain command and control, exfiltrate data, or redirect web traffic. When internet requests are resolved by a recursive DNS service, they become the best place to check for and block malicious or inappropriate domains and IPs. DNS is one of the most valuable sources of data within an organisation and can be used to cross-reference against threat intelligence.

New analysis shows widespread DNS protection could save organisations as much as $200 billion in losses every year. *The Economic Value of DNS Security*, recently published by the Global Cyber Alliance (GCA), found that DNS firewalls could prevent between $19 billion and

Cisco Systems Australia Pty Ltd

Level 14, 101 Collins Street

Melbourne Victoria Australia 3000

$37 billion in annual losses in the US and between $150 billion and $200 billion in losses globally.

DNS type technology solutions that use the internet's infrastructure to stop threats over all ports and protocols before it reaches endpoints or network can proactively block connections to malicious destinations at the DNS and IP layers. This would be an effective way to reduce high volume and low sophistication cyber threats. It is a fast and easy mechanism for companies and organisations to bolster their security defence and forensics capabilities.

Some businesses are already seeing value in ensuring that their customers are appropriately aware of cyber threat risks and how best to mitigate and manage them. National Australia Bank recently released a small business cyber security handbook, *Your business and cyber security*, which complimented the Australian Cyber Security Centre's, *Small Business Cyber Security Guide.* These assets are valuable contributions to the ongoing improvement in SMBs cyber threat posture and demonstrate a positive, proactive and cooperative approach from business and government working together. National Australia Bank is also offering discounted cyber security products to its small business customers as an incentive to get them to be more cyber aware and secure.

Key Recommendations:

- Provide guidance on minimum standards for small business to follow (DNS/firewall security, locked & encrypted laptops etc)

Supply chain security

In our increasingly digital world, technological innovation not only presents new opportunities, but also raises new risks and challenges that must be addressed collaboratively by industry, buyers, users, and policymakers.

Specifically, digitization demands that risk be addressed across a dramatically expanding supply chain. These risks include the security threats of manipulation, espionage and disruption of information and information systems and services.

Empirical reports reveal that the third party ecosystem remains a fundamental risk to the integrity of our information systems. For example, analysis of the last nine consecutive years of Verizon's global Data Breach Investigation Reports illustrates that where breaches can be

Cisco Systems Australia Pty Ltd

Level 14, 101 Collins Street

Melbourne Victoria Australia 3000

attributed, 73% arise from the third party ecosystem. Not only are we increasing the volume of third parties in our information systems supply chains, we continue to invite third parties into our security inner sanctums – our security enforcing technology. *Cisco's 2018 Annual Cybersecurity Report* revealed that 79% of global enterprises and governments rely on at least 20 third party security vendors, dramatically highlighting the cyber supply chain and its related third-party risks that must be addressed.

Exploits in supply chain have been leveraged successfully in the past, from targeted social engineering attacks to authorise fraudulent vendor payment, to vendor access compromise, including credential compromise and using their equipment as pivot points into enterprises.

For Cisco's part as a third party in our customers supply chains, we are committed to maintaining strong protections for our customers, products, and company. This starts with an awareness of business dependencies, from physical premises to third parties and supply chains. This is a structure worth following particularly when it comes to identification and leveraging strong multi-factor authentication. SMS as one of those methods should be considered weak.

Security risks must be tackled comprehensively across all stages of the supply chain, including design, software development, manufacturing and sustainment. In parallel, procurement practices, policies and certification and validation schemas should also seek to mitigate the impact of this third-party risk.

Public-private partnership brings civilian, government and defense agencies together with private industry to develop meaningful recommendations to effectively mitigate third party risk. NATO has recognized and is actively addressing this challenge in coordination with its member nations.

Pervasive Security is a concept developed and designed to deploy a layered approach balancing physical security, operational security, behavioural security, information security and security technology across the cyber supply chain based on risk prioritization. NATO's 2017 Technical and Implementation Directive on Supply Chain Security for COTS CIS Security Enforcing Products, is the basis for pervasive security and can act as a practical framework to identify, prioritize and mitigate the impacts of tainted and counterfeit information systems technology across the supply chain and its third-party members.

Cisco Systems Australia Pty Ltd

Level 14, 101 Collins Street

Melbourne Victoria Australia 3000

Risk travels up and down the supply chain. Approaching supply chain security comprehensively is key to ensuring successful risk management. The fundamental steps to comprehensive security require that all supply chains are evaluated to:

1. Identify areas of potential impact, for example, risks to continuity of supply of third party provided software, services, components and raw materials, natural disasters, geopolitical and economic disruption, workforce instability, financial volatility, weak infrastructure security, and insufficient end-user risk awareness
2. Prioritise risk by both likelihood of occurrence and severity of impact
3. Establish criteria for mitigating security threats and reducing the impact of incidents, and
4. Collaborate with industry and government on policy, regulations and directives.

Key Recommendations:

- Establish supply chain security through education efforts
- Develop and promote supply chain security risk management frameworks appropriate for different sectors and organisational sizes

Improving consumer awareness about cyber security

An informed and educated consumer about the cyber threat landscape could be the most efficacious program that government could initiate.

This could begin by setting an ambitious goal or target; for example, to make Australia the cyber-safest place to live and do business in the world, with informed citizens able to understand and identify possible cyber security safety risks and attacks.

Broadly educating citizens about cyber safety and risks is a challenging task but there are existing, freely available resources that could help to improve consumer awareness about cyber security.

Identity is becoming increasingly mutable. More online data, combined with advancing impersonation capabilities (e.g. deep-fake video) means stronger authentication capabilities are mandatory

Cisco Systems Australia Pty Ltd

Level 14, 101 Collins Street

Melbourne Victoria Australia 3000

For consumers, managing passwords and dealing with a myriad of sites often leads to password re-use. Password managers and similar technologies are a must. For key accounts (banking/email/govt/health) users should have multi-factor capabilities.

Federal and state governments could help play a leading role in educating citizens simply by providing basic cyber security training for the more than 1.2 million public servants around Australia. Many businesses require staff to undertake mandatory OH&S training or Code of Business Conduct training which must be refreshed each year. These courses are usually compulsory as part of employee induction programs or compliance and risk assessments. Cyber security training could also be made mandatory or part of an induction program for Australia's public servants.

Key Recommendations:

- Implement nationwide recommendations and tools to keep consumers safe
- Set an ambitious goal for Australia as a cyber secure nation with educated citizens
- Federal and state government employees to undergo basic cyber security education and training

Towards better information sharing between government and industry

It has long been noted that cybercriminals are better organised than those that need to defend against them. A key aspect of that is intelligence sharing. Exploits are traded far more easily, widely and quickly than threat intelligence.

The government can play a key role in assisting to accelerate and simplify threat intelligence sharing by building on existing frameworks and processes. Issues of timeliness, trust and veracity can be handled on a sector by sector approach.

Cisco recognises the progress of threat intelligence sharing initiatives to date such as the JCSC however as in 2016, we recommend a focus of achieving this at "machine speed" and that intelligence is "actionable intelligence". Given the diminishing window between vulnerable knowledge and exploit "in the wild" of that vulnerability, we need to focus more so than ever on this sharing happening at machine speed.

Equally as important is the ability of organisations to act based on that knowledge. This is an area where government and industry could work closely together to address the needs and

capabilities of both large and small organisations as well as Australia citizens. Large organisations with mature security teams can use threat intelligence in their threat hunting and detection capabilities – injecting into their own monitoring systems for example. Smaller organisations however would be challenged to do this, and the most pragmatic outcome is for their security product vendors and security MSPs to do this on their behalf. In short, they are protected by vendor provided updates to the products they run.

Threat intelligence curated or disseminated by the government should be shared not only with critical industries or other sectors but also directly to the cyber security industry so it can be included in their product updates – ultimately protecting Australian business and citizens.

An industry advisory committee with key cyber industry players is recommended to help shape this framework and process.

Key Recommendations:

- Implement industry specific threat intelligence sharing framework appropriate to organisational size and sector – including the cyber security industry itself.

Tackling cyber skills shortages

Government and industry are working together constructively and closely on initiatives designed to tackle the cyber security skills shortages.

Following the 2016 recommendation to develop TAFE courses in Cyber Security, Cisco was pleased to be involved in the industry advisory group for the development of Certificate IV and Advanced Diploma courses with the Box Hill Institute, certifications which AustCyber helped facilitate into a national program.

In parallel, Cisco has invested heavily in the Cisco Networking Academy Program (which provides some coursework for these new TAFE certifications). This is specifically focussed on training students in job-ready cyber security skills. Cisco also recently partnered with Victoria University St Albans Campus to invest in a cyber security training centre which is attracting students from that region of Melbourne and from other industries who are looking to reskill.

One area for government consideration is to again investigate the specific detail of the cyber skills shortage to allow for more effective resource allocation and education and training focus. In the intervening period since the 2016 report, a significant number of cyber security training courses are now on offer in both VET and University sectors. Before calling for further training initiatives, developing reliable, consistent and current metrics on the shortfall of cyber security professionals in Australia by region will also allow industry to better understand the role they can play in supporting and investing in programs to help tackle those shortages.
Additionally, consideration should be given to tackling the root cause of a lack of cyber security rather than too much focus on just the job roles dealing with the problems caused by a lack of cyber security. Addressing privacy by design and secure development practices for both software and hardware are example of areas where education and skilling might help reduce security problems earlier on rather than trying to resource the problem at the end.

Key Recommendations:

- Understand the resource shortfall in more detail including opportunities to teach cyber security skills and knowledge in a proactive rather than reactive manner.

Leading by example

An opportunity exists for the government to continue to implement strong regulation and accountability for security and privacy of all government entities. Establishing citizen trust in the collection and handling of data is essential. Security and privacy by design should by the guiding policy for all government ICT systems as a pathway toward building trust to enhance community uptake and acceptance of digitisation.

Policy and regulatory implementation must be adequately resourced. In Cisco's 2016 submission, we made the following observation:

> *The pace of these cybersecurity threats is increasing as fast, or likely, faster than the technology development cycle, which in turn is moving much faster than the currently complex compliance and policy vehicles. Initiatives that address the difference in pace, through simplicity and scale, are critical if the Internet, and ICT systems in general, are to deliver maximum benefit to organisations, society, and countries.*

Cisco Systems Australia Pty Ltd

Level 14, 101 Collins Street
Melbourne Victoria Australia 3000

As we approach 2020, the shift to subscription-based consumption models across industry and the move to cloud first or cloud only delivery, has seen programs such as the CCSL become virtually closed for accepting any new SaaS certifications. As the use of SaaS applications continues to accelerate, CCSL and similar programs must keep up with demand or risk being a drag on the digital economy. Industry consultation is needed before adopting a similar approach in other sectors or technology domains.

As examples, self-attestation or adopting international rather than national certifications and accreditations should be considered. We cannot allow the pace of certification to impact establishing cyber resilient posture in products and services.

With the advent of quantum computing around the corner, Australia must be ready to adapt to quantum resistant encryption technology. This has impact in several areas including authentication capabilities, but particularly with regard to certification as we look at new key sharing schemas, for example, to address the challenge.

Globally, successful regulation includes reporting and non-compliance/breach penalties. GDPR for example has been a driver of a focus on privacy and cyber security.

Key Recommendations:

- Bolster security incident disclosure regulations
- Implement appropriate privacy regulation
- Investigate how to close the gap between the pace of technology and the pace of current certification regimes

List of attachments:

Cisco 2019 Asia Pacific CISO Benchmark Study Report
Defending against today's critical threats: February 2019 Threat Report
Cisco 2020 Global Networking Trends Report