A Call for Views - Australia Cyber Security Strategy 2020 - Schneider Electric Submission - 301019

	QUESTION	RESPONSE
1	What is your view of the cyber threat environment? What threats should Government be focusing on?	The key point is that the cyber threat environment is constantly evolving - becoming increasingly more aggressive and sophisticated. The priority threat focus is threats to critical infrastructure and supply chain - because of the severe social, political and economic consequences. However the government needs to be involved in all areas of cyber security, as individuals and small businesses do not have sufficient resources or knowledge to adequately defend themselves. Supply chain regulation, and cyber services contractors regulation are also key concerns.
2	Do you agree with our understanding of who is responsible for managing cyber risks in the economy?	The responsibility of cyber risk management is effectively shared by the business (or institution) itself, secondly by the goods and services providers to the business, thirdly by the consumer, and supported by government. The key concern here is that there are huge differences in the maturity and abilities of businesses in their cyber security strategies and skills.
3	Do you think the way these responsibilities are currently allocated is right? What changes should we consider?	For large businesses, the responsibility of cyber risk for will remain primarily with the business itself, as a core element of operations stability and as a business imperative for protecting their own customers. For small businesses, the government needs to assume more responsibility for protecting and regulating them both as being consumers and providers of goods and services. For individuals, the government needs to assume close to total responsibility to protecting and educating them as consumers, as they have virtually no capability to discern the cyber security risk of goods and services.
4	What role should Government play in addressing the most serious threats to institutions and businesses located in Australia?	Specifically for critical infrastructure, the government needs to continue all current programs, but the key area for critical infrastructure is faster national threat responses, and fostering more open threat intelligence sharing. This looks like it might require mandatory threat reporting, especially for critical infrastructure. Additionally more "sector specific" programs will help to practically drive efficient appropriate minimum security defense across different sectors with different needs.
5	How can Government maintain trust from the Australian community when using its cyber security capabilities?	Government can maintain and improve support and trust through constant community and industry consultation and collaboration, public communication, highlighting successes.
6	What customer protections should apply to the security of cyber goods and services?	Companies should have public cyber security capability ratings and competency certifications. These should be formally regulated.
7	What role can Government and industry play in supporting the cyber security of consumers?	1. Better regulation of supply chain of goods and services. 2. Products should have cyber security ratings - so that consumers can easily understand cyber security quality of goods 3. Certification of contractors and service providers 4. Consumer education.
8	How can Government and industry sensibly increase the security, quality and effectiveness of cyber security and digital offerings?	1. Improve security of the supply chain 2. Increase support for sector and collaboration groups 3. Increase market of cyber security professionals 4. Certification system
9	Are there functions the Government currently performs that could be safely devolved to the private sector? What would the effect(s) be?	The considerations for devolving are who and what. Government can devolve cyber security functions through "sector" specific groups. Sector specific groups can manage and decide on cyber security policy and frameworks for their sector.
10	Is the regulatory environment for cyber security appropriate? Why or why not?	The most efficient and effective regulatory environment occurs when alignment exists between regulating bodies. There are frequently differences in compliance and enforcement, which places unnecessary overhead on businesses and institutions.

11	What specific market incentives or regulatory changes should Government consider?	Market incentives (tax, grants) for R&D, minimum compliance programs. Regulatory changes: Mandatory threat reporting for major incidents and critical infrastructure. Consider a roadmap towards IEC62443 as a mandatory standard for new control systems implementation and operations.
12	What needs to be done so that cyber security is 'built in' to digital goods and services?	Secure Development Lifecycle (SDL) should be followed by all manufacturers. Product certification (example: Achilles cert or equivalent) Contractor certification program. Accelerate service providers certification achievement.
13	How could we approach instilling better trust in ICT supply chains?	Certification and compliance programs are necessary.
14	How can Australian governments and private entities build a market of high quality cyber security professionals in Australia?	Support education, re-education, upskilling across the market. Build a more sophisticated market including more startups, R&D.
15	Are there any barriers currently preventing the growth of the cyber insurance market in Australia? If so, how can they be addressed?	Barriers to cyber security market are the unknowns and dependencies on the customer side, which makes it challenging to offer competitive insurance. Cyber events are risky and somewhat inefficient to insure because they are low probability and very high consequence. These could be addressed in part by adherence development of insurance standards, independent cyber defence testing and certification, and common insurance pool.
16	How can high-volume, low-sophistication malicious activity targeting Australia be reduced?	Stronger international partnerships to pursue perpetrators globally. Better intelligence and information sharing. Better collaboration with industry, institutions, ISPs and online providers.
17	What changes can Government make to create a hostile environment for malicious cyber actors?	Cyber security basic applications installed universally to achieve baseline protections. Increase public vigilance through awareness and education. Increase automatic detection through more sophisticated technologies such as AI. Find and pursue the sources and increase penalties. Publicise prosecutions.
18	How can governments and private entities better proactively identify and remediate cyber risks on essential private networks?	Better intelligence sharing (systems and procedures) Strongly consider mandatory threat reporting
19	What private networks should be considered critical systems that need stronger cyber defences?	All critical infrastructure, critical services, critical buildings, finance, communications networks, some supply chain, some environmental, some data centres. Power and utilities, transport, banking, medical, critical resources (food, fuel, medical supplies), defence related private companies.
20	What funding models should Government explore for any additional protections provided to the community?	Funding collaborative industry groups, startups, R&D.
21	What are the constraints to information sharing between Government and industry on cyber threats and vulnerabilities?	For fast response to critical attacks, use trusted private member communication groups sharing suspected threats (unverified). Rate threats by severity and degree of certainty. Threat information updated as situation develops. Verified threats would then be publicly communicated at large. Reporting of critical attacks on critical infrastructure should be mandated - but easily reportable without placing a burden on reporter.
22	To what extent do you agree that a lack of cyber awareness drives poor consumer choices and/or market offerings?	Poor cyber awareness simply prevents consumers from identifying products and services with poor cyber security, or understanding the consequences of poor cyber security choices. A cyber quality rating system printed on products would help consumers immensely.

23	How can an increased consumer focus on cyber security benefit Australian businesses who create cyber secure products?	Consumer focus on cyber security would create an informed discerning customer who would choose products with better cyber security.
24	What are examples of best practice behaviour change campaigns or measures? How did they achieve scale and how were they evaluated?	Best practice behaviour change has a strong human element - very memorable messages and stories that are personal and resonate. They also give clear direction on what to do and how to act. They are often close to the point of action. Early education is crucial as behaviour change is generational too.
25	Would you like to see cyber security features prioritised in products and services?	Establish cyber security quality ratings - for consumer products (5 star, etc), for industrial/commercial technology Mandate cyber security certifications - for service providers, contractors, cyber professionals
26	Is there anything else that Government should consider in developing Australia's 2020 Cyber Security Strategy?	There is a lot of focus on critical infrastructure at the big end and the consumer at the individual end. There are very many significant large companies classified as non-critical, that are very exposed to cyber crime, and bear some of the largest financial losses. These companies are often non-compliant to any standards, and this tier would benefit from more focus and scrutiny.