Australia's cyber security strategy 2020 – Submission Form

What role can Government and industry play in supporting the cyber security of consumers?

How can high-volume, low-sophistication malicious activity targeting Australia be reduced?

Taking necessary steps including compliance directives (e.g time for putting remediation measures in place on specific attacks) that drive private sector service providers (e.g. ISPs) to build and maintain the systems capability to prevent high volume, low complexity attacks.

Targeted information campaigns that educate on risks and threats for consumers

What specific market incentives or regulatory changes should Government consider?

Driving industrywide security standards adoption with sector specific incentives and regulation, especially in sensitive sectors like energy and transport.

How can Australian governments and private entities build a market of high quality cyber security professionals in Australia?

Clarity on career pathways, support for more apprenticeships (post graduate and Ph.D level) in the area with incentives for academia - industry collaboration, initiate dialogue with leading players in critical Australian business sectors to better understand security environments they operate in and forming education and skills development policies accordingly. Continued support & incentives for global talent to fill any critical skill gaps.

What private networks should be considered critical systems that need stronger cyber defences?

Energy systems networks, transportation systems, healthcare systems.

How can an increased consumer focus on cyber security benefit Australian businesses who create cyber secure products?

Development of home market for such products and services due to increased consumer focus will lead to more participation by the private industry in Australia and indirectly drive demand & growth of skills

Would you like to see cyber security features prioritised in products and services?

Yes.