Submission in response to

Australia's 2020 Cyber Security Strategy

Public Version

November 2019

INTRODUCTION

1. Optus welcomes the opportunity to provide a submission to the Department of Home Affairs Discussion Paper *Australia's 2020 Cyber Security Strategy*. Optus considers the release of this Discussion Paper is timely given the ever-increasing cyber threat landscape.

2. As a technology leader, Optus observes the all-pervasive impact that technology has had on the everyday lives of Australians and the wider economy. Indeed, for many Australians a high percentage of their work and leisure activities are undertaken using digital platforms. The security of these platforms is therefore paramount.

3. This Optus submission does not seek to provide answers to all questions posed in the Discussion Paper, but rather offer some general insights that will go to the points raised in the paper.

4. Optus considers that the overarching challenges for Government in ensuring a secure cyber environment relate to a general unawareness/preparedness of end users and organisations, and a shortage of relevant cyber skills.

   (a) The sheer number of connected devices means that there are an almost infinite number of possible combinations to establish an end-to-end data connection. This in turn creates many different layers and responsibilities in the creation of a secure cyber experience. Optus welcomes a discussion of this increasing complexity but considers that it should be undertaken in the context of security literacy for all users and asset owners.

   (b) Underpinning the security of Australia's cyber environment is a skilled workforce. Optus contends that Australia faces a current skills shortage for appropriate cyber qualifications which will only magnify future issues without intervention.

5. Optus considers that the Government's role is to sit over the top of this sphere of activity and provide an education and alert service, as well as to deliver programs to increase the number of skilled cyber security workers.

6. Further, Optus observes that the blurring of lines between cyber security, national security and online safety generates additional challenges for government in ensuring a safe online experience for all. Optus therefore recommends that this strategy be considered in the broader context to either clearly delineate cyber security, or clearly articulate the linkages between the issues.

7. Finally, Optus considers that the use of a prescriptive legislative framework in a rapidly evolving environment such as cyber security is not appropriate, as there would be a lack of flexibility to accommodate technology change. However, we do see a need for industry codes and standards to ensure all providers have access to minimum standards.

8. Optus would welcome the opportunity to discuss any aspect of this submission in further detail.

Optus background

9. Optus is a global leader in cyber security given our unique position in the market place. In the first part of 2019, Optus brought together the assets and people of Optus Cyber, Trustwave and Hivint into one brand – Trustwave, an Optus company.

10. Trustwave is a leading cybersecurity and managed security services provider that helps businesses fight cybercrime, protect data and reduce security risk. Offering a comprehensive portfolio of managed security services, consulting and professional services, and data protection technology, Trustwave helps businesses embrace digital transformation securely. Trustwave is a Singtel company and the global security arm of Singtel, Optus and NCS, with customers in 96 countries.

11. For multiple years running, Trustwave has been named in Gartner's leaders quadrant for vendor performance in the cyber security space. It has also been recently named as a leader in the Asia-Pacific region. Trustwave's capability covers the entire lifecycle of a security incident–from initial detection through returning a network back to steady state operation—due to its global team of security professionals.

Roles and responsibilities

12. Today's digital technologies are enabled by a resilient, secure and reliable communications infrastructure. However the line between the underlying physical network layer and the application layer is increasingly blurring with the presence of over the top players, non-traditional carriers entering the market and prevalence of in-house network assets.

13. The myriad of potential applications, devices and networks that data can be sent across generates several layers of complexity and takes cyber awareness away from being the sole domain of carriers and large enterprises into a genuine information need for all Australian individuals and enterprises.

14. Optus cooperates closely with government agencies in many areas to avoid or minimise the impact of cyber incidents. As a carriage service provider, Optus is also required to comply with obligations to make our networks resilient from unauthorised access and interference and to main competition supervision and control of networks and systems.

15. Optus has observed over recent years a tendency to shift responsibility for addressing cyber security onto the providers of such infrastructure. While it is clear that Optus has a role to play in protecting its own assets, it is not possible for telecommunications carriers to make any meaningful changes to networks and systems outside our control, indeed Optus contends that it would be highly inappropriate to raise this as an expectation.

16. For example, end user devices such as a PC or laptop are high risk vectors for cyber vulnerabilities and could be sourced from any number of vendors, with an equally large number of potential software applications installed on the device. It is not possible for a telecommunications carrier providing a simple connectivity service (such as a broadband connection) to be able provide any meaningful level of security on the device in such a situation.

17. Similarly, at the enterprise level it would be wholly inappropriate for the organisation to expect a telecommunications carrier to ensure its internal systems are secure without a commercial arrangement for that specific service.

18. Cyber security therefore requires an industry, user and government approach to collaboration given the varied elements and stakeholders. Optus would consider a broad set of principles could be structured as follows:

    (a) Telecommunications operators should be responsible for the security and resilience of their networks and the services they provide to users.

(b) Government should be responsible for ensuring telecommunications operators, and operators of critical services to take measures to safeguard networks and services, as well as providing an alert service for serious vulnerabilities and educating users on basic IT security.

(c) Users (ranging from large enterprise to individual), should be responsible for educating themselves on the device combinations being used in their networks, including home networks, and the resulting vulnerabilities/treatments in the same way that physical security of buildings is the responsibility of the building owner/user.

19. Optus notes that this will be particularly challenging for individuals or small-medium enterprises, who do not have the capabilities to either perceive the risks of cybercrime or to implement the required security mechanisms.

20. Optus considers that a coordinated Government-led education campaign is required to raise awareness and increase security literacy of all Australians, particularly at the lower-resourced end of the market. Current information resources require an individual to actively search for information rather than a push to the general public.

The cyber security skills gap

21. Optus contends that one of the greatest challenges posed by cyber security is the constant need for expert resources to cope with expanding threats. This demand for specialists is not met with an equal supply to all Australian enterprises and is being exacerbated by the competition from other sectors (such as financial services).

22. In recognition of this, in 2016 Optus announced a $10 million investment in the Optus Macquarie University Cyber Security Hub to form a network of academic, business and government leaders:

(a) Providing expertise and leadership in cyber security regarding technology, governance, policies and human factors;

(b) Offering a platform for exchange between academics and practitioners from business and government;

(c) Conducting cross-cutting research across several disciplines: computing, engineering, business, criminology, law and psychology; and

(d) Training the next generation of cybersecurity specialists as well as raising awareness among our leaders and developing the skills of the existing workforce.

23. In addition, Optus has partnered with La Trobe University to create a digitally connected campus as well as a market leading cyber security tertiary degree.

24. Notwithstanding these partnerships, there is far more work to be done to ensure that the skill shortage is closed, particularly noting the impending explosion of devices due to the rollout 5G and greater usage of the Internet of Things.

25. Optus considers that there is an urgent need for the Government to review the adequacy of cyber security education pathways, and what incentive programs can be implemented.

Regulatory frameworks

26. Optus considers that the use of a prescriptive legislative framework and rules-based regulation in a rapidly evolving cyber security environment is inappropriate as they lack flexibility to accommodate technology change.

27. However, we see a need for well-developed industry codes, standards, and best practices to ensure that there is an understanding of the minimum standards for business and individuals in considering how to secure their digital activities.

28. Noting previous comments around the blurring of lines between cyber security, national security and cyber safety, there is a real risk that uncoordinated efforts will lead to differing security environments, increasing the complexity of creating secure networks. It is essential therefore that all stakeholders, including those outside the traditional tech industries who may be hosting in-house networks or digital assets, work together to set common and open security standards.

[ENDS]