Strengthening Australia’s Cyber Security Regulations and Incentives

Submission by Fortinet, Inc.
27 August 2021

Background on Fortinet

Founded in 2000, Fortinet, Inc.[1] (Fortinet) is a US-based developer of next generation security and networking solutions and architectures. Fortinet is the most innovative provider of cybersecurity with over 700 patents, and is focused on protecting the breadth of the digital attack surface from edge to core to cloud.

Fortinet's broad, complementary portfolio of cybersecurity solutions is built with integration and automation in mind, enabling more efficient, self-healing networking, security operations and rapid response to known and unknown threats, helping us achieve our mission to secure people, devices, and data everywhere. Fortinet's high-speed network security microprocessors are proudly designed in the United States, and the vast majority of our R&D is performed in the U.S. and Canada.

Fortinet is the only security leader to develop and build custom security processing unit (SPU) technology to offer the best performance and cost value in the industry. Fortinet's FortiGuard Labs uses one of the most effective and proven artificial intelligence (AI) and machine learning (ML) systems in the industry to process and analyse more than 100 billion events daily, sending actionable real-time threat intelligence to customers.

Fortinet is a trusted partner across many industries in Australia, ensuring the safety, security, and reliability of a wide variety of the country's most critical infrastructure. We have an active Common Criteria program of work and develop solutions certified for use by all Five Eyes countries. Fortinet invests heavily in the Federal and Defence market in Australia, including investment in local capability and cleared resources to ensure that our solutions are built to serve the Australian Government. In fact, Fortinet is establishing an Innovation and Integration Centre (IIC) in Canberra to provide sovereign cybersecurity services, customer proof of concept (POC), technical analysis, and SME collaborative opportunities.

Partnering and collaborating with both the public sector and industry has been a cornerstone of Fortinet's strategy for many years. We are a founding member of the Cyber Threat Alliance (CTA) and the World Economic Forum's Partnership against Cybercrime, two of the leading global forums for cybersecurity collaboration. We strive to ensure a secure and productive economy for all by working with industry, CERTs, government, and academia to share threat information and protection to raise cyber resilience.[2]

[1] About Us, Fortinet, https://www.fortinet.com/corporate/about-us/about-us (last visited Aug. 26, 2021).
[2] Fortinet is also a member of the Information Technology Industry Council (ITI).

Executive Summary

Fortinet respectfully submits these comments in response to the Australian Government's Call for Views on "*Strengthening Australia's cyber security regulations and incentives*" (Call for Views). Fortinet appreciates the opportunity to provide its thoughts and perspectives on these issues of utmost importance.

Fortinet supports the Government's efforts to strengthen cyber security for all Australian businesses. We believe the goal "to make Australia's digital economy more resilient to cyber security threats"[3] is a goal shared with the private sector and we support the creation of "stronger incentives for Australian businesses to invest in cyber security."[4] We hope this critical and timely process results in a balance of government incentives, policy reforms, and strengthening of public-private partnerships to improve cyber resilience across the economy. Furthermore, clarity and simplicity in cyber policy will enable small, medium, and large businesses across all sectors to more effectively combat malicious cyber activity.

There has been a surge in the sophistication and volume of advanced cyber security threats over the past few years. Fortinet's recent Global Threat Intelligence Report found a 10.7x increase in ransomware over the last 12 months.[5] In fact, we found that "the first six months of 2021 have seen wide-scale attacks that spread to envelop numerous organisations and countless individuals become a regular occurrence."[6] The threat ecosystem is becoming more sophisticated, and threat actors now routinely deploy machine learning and artificial intelligence to exacerbate both the scale and the impact of the cyber threat. The threat has evolved alongside accelerated digital transformation driven by the COVID-19 pandemic, with endpoints, networks, Internet-of-Things (IoT) devices, cloud environments, and Operations Technology (OT) targeted in equal measure – at times with devastating real world consequences.

The Government's thoughtful review and action in this area will help strengthen the digital economy and protect the digital presence of all Australians.

[3] *Strengthening Australia's cyber security regulations and incentives: A Call for Views*, Department of Home Affairs, at 2 (July 13, 2021), https://apo.org.au/sites/default/files/resource-files/2021-07/apo-nid313193.pdf ("Call for Views").

[4] *Id.*

[5] *Global Threat Landscape Report: A Semiannual Report by FortiGuard Labs*, Fortinet, at 3 (Aug. 2021), https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/report-threat-landscape-2021.pdf.

[6] *Id.*

Detailed Responses

For the purposes of this response, Fortinet provides its responses to the key questions in the Call for Views below.

Question #1: What are the factors preventing the adoption of cyber security best practice in Australia?

Presently, Fortinet believes two of the factors preventing the adoption of cyber security best practice in Australia are the lack of information security awareness and incentives available to small to medium sized businesses.

Adoption of best practices across the country would benefit from the strengthening of information security awareness within the public, development of a more robust cyber workforce, and targeted government incentives to increase the pace and extent of progress.

Fortinet believes that the Government should focus on increasing training opportunities in partnership with educational entities and the private sector. Building a strong cyber aware population will complement efforts to protect and expand the digital economy. Whether it is the local florist, a startup entrepreneur, or a mid-sized firm, foundational knowledge of how and why it is necessary to protect a businesses' systems and data would complement incentives to achieve robust cyber resiliency.

The Australia's Cyber Security Strategy 2020 report noted the need for broad engagement and awareness via targeted support to the education sector,[7] and great steps have been taken with initiatives like the Cyber Security Cooperative Research Centre. There remains an opportunity to expand the reach to the primary and secondary school systems for earlier interaction and education on the threats and opportunities that cyber brings to Australians.

Fortinet believes the Government should also act to bolster creation and growth of cyber talent generally. The existing cyber security skills gap presents challenges to both private sector security vendors innovating to stay ahead of the threat actors, and also to the small and medium businesses that need this talent to protect their systems and data.

It is Fortinet's view that Government investment, through incentives to small and medium businesses coupled with policy geared toward these entities, would ensure that cyber resiliency extends beyond large companies and government.

[7] Australia's Cyber Security Strategy 2020, Department of Home Affairs, at 33 (Aug. 2020), https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf.

Question #5: What is the best approach to strengthening corporate governance of cyber security risk? Why?

Fortinet agrees with the Government's recognition that any action in this space should be "proportionate, achievable, and internationally consistent".[8]

Standards need to be implemented and managed within the context of the business environment, with a focus on the sensitivity of the data held, the impact of any breach on data confidentiality/integrity/availability, the threat landscape, the resources available, and the return on investment from implementation.

Question #6: What cyber security support, if any, should be provided to directors of small and medium companies?

Fortinet believes that action by small and medium companies would benefit from Government incentives and broader availability of information security training for directors and all employees. Many of these business leaders are operating in an information vacuum, and would benefit from the Government providing information and resources to enable creation of baseline levels of cyber capability and understanding in the small and medium-sized business community across sectors.

Question #7: Are additional education and awareness raising initiatives for senior business leaders required? What should this look like?

Yes. Fortinet believes that the Government's 'stay smart online' campaign is useful and impactful, in part because it is aimed at individuals and small businesses. Approximately 98% of Australia's economy is comprised of "small businesses".[9] Significantly, small businesses are much less resourced and cyber mature, and are very exposed to cyber threats like ransomware. For the Government to work with industry to expand the scale and scope of the Stay Smart Online program presents a tremendous opportunity.

Businesses should be incentivised to leverage quality cybersecurity awareness, tools and training resources. This material should also be built into general employee training. The Government can partner with private sector entities who already boast mature, quality cyber training resources to establish a prominent, central repository for Australian business to access these resources.

[8] Call for Views at 20.

[9] Small Business Counts December 2020, Australian Small Business and Family Enterprise Ombudsman, at 5 (Aug. 2020), https://www.asbfeo.gov.au/sites/default/files/ASBFEO%20Small%20Business%20Counts%20Dec%202020%20v2.pdf.

Question #11: What is the best approach to strengthening the cyber security of smart devices in Australia? Why?

Zero Trust[10] is a good foundational approach that Fortinet would recommend to apply here. Zero Trust is the term for an evolving set of cybersecurity paradigms that move defences from static, network- based perimeters to focus on users, assets, and resources. Zero Trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned). The concept of Zero Trust is well articulated and widely understood, has strong implementing guidance and principles, and can help to integrate smart device cybersecurity with broader national cybersecurity priorities. Adoption of Zero Trust is growing globally as evidenced in the recent United States *Executive Order on Improving the Nation's Cybersecurity.*[11] The Zero Trust approach poses significant opportunity to compliment the Essential 8 as best practice advice.

It is Fortinet's view that strengthening cyber security on smart devices can only be successfully implemented as part of a broader, national framework. Having a standard reflecting a range of risk and regulations on what can be deployed and where it can be deployed would be an optimal outcome. For example, using low cost, insecure, smart movement sensors on a cattle farm would theoretically pose little risk since deployment is in a dedicated segment of a rural system. However, these sensors should not be used on the sensitive internal network of a bank or government or council premises, where a sensor with a higher level of protection rating would be required.

Question #16: What is the best approach to encouraging consumers to purchase secure smart devices? Why?

Fortinet believes that education and context are key to encouraging and enabling better consumer buying choices. Greater public cyber awareness is needed to guide consumer thinking and create market demand. Guidance on the intended use of certain devices and appropriate locations or environments of use would also help consumers. There are many cases where a cheap, disposable smart device is viable and perhaps the most affordable and desirable choice for consumers. Conversely through education, the consumer would also be able to how to identify when and under what circumstances to purchase and use devices with built-in security because of a greater level of risk.

Question #17: Would a combination of labelling and standards for smart devices be a practical and effective approach? Why or why not?

Yes. Fortinet believes that a combination of labelling and standards would be both practical and effective. As proven in many other sectors (such as in the technology sector), consumer labelling information is a practical way to reach consumers and enable them to make informed

[10] Peter Newton, *Zero Trust Security: Definition and Key Principles*, Fortinet (Feb. 18, 2020), https://www.fortinet.com/blog/business-and-technology/know-who-and-what-with-zero-trust-network-access.

[11] Executive Order No. 14028, 86 Fed. Reg. 26633, 26635-36 (May 17, 2021).

decisions about prospective purchases. It provides an opportunity for consumers to consider and compare cyber security solutions at the time of purchase. These efforts should be coupled with greater cyber awareness for the public to fully utilise and understand the labels. The Government should also strive to harmonise any adoption of labelling and standards efforts with international partners.

Question #19: Would a security expiry date label be most appropriate for a mandatory labelling scheme for smart devices? Why or why not?

Under certain circumstances, yes. Fortinet believes this is a valid idea if synchronised to reflect when a manufacturer deprecates support for any particular product. This is important because as technology becomes older and support diminishes or ceases, it generally becomes easier to exploit from a cyber security perspective. However, this should not detract from the end user's responsibility to update software and apply security patches where applicable.

Question #21: Would it be beneficial for manufacturers to label smart devices both digitally and physically? Why or why not?

Fortinet would recommend some form of digital label that provides an indication of risk based on hardware, operating system, patch level, and installed applications would be the most effective approach. Digital labelling could also be dynamic, reflecting changes in protection based on the evolution in standards and potentially in threat capability.

Question #25: Is there anything else we should consider in the design of a health check program?

Fortinet agrees with the Government's perspective that a successful program would require incentives to small businesses to encourage broad participation.[12] Incentives for a program focused on diagnosis should not distract from incentives to address actual gaps in systems and processes. With limited capital and time to devote to cyber security, simplification of the program for small businesses, including easy access to cyber security experts for implementation, should also be considered.

We also agree with the Government's recognition to avoid a 'set and forget' approach.[13] With rapid innovation in cybersecurity as well as advances from threat actors, the program should have the flexibility to evolve over time.

[12] Call for Views at 50.
[13] Id. at 48.

Conclusion

Thank you for the opportunity to contribute to the important discussion on strengthening Australia's cyber security policies. Fortinet stands ready to discuss these comments in further detail and looks forward to the continued opportunity to work with the Government to bolster the cyber resiliency of the economy.

Should you have any questions, please don't hesitate to contact Lisa Musladin, Federal Government Branch Manager ([redacted]) or Hugh P. Carroll, Head of Government Affairs ([redacted]).