REQUEST FOR COMMENT

2023–2030 Australian Cyber Security Strategy: Legislative Reforms Consultation Paper

March 1, 2024

I. INTRODUCTION

In response to the Australian Government's request for comment ("RFC") on its 2023-2030 Australian Cyber Security Strategy: Legislative Reforms Consultation Paper ("Consultation Paper"), CrowdStrike offers the following views.

We approach these questions from the standpoint of a leading international, US-headquartered, cloud-native cybersecurity provider that defends globally distributed enterprises from globally distributed threats. CrowdStrike offers insights informed by multiple practice areas: cyber threat intelligence; proactive hunting, incident response and managed security services; and an AI-powered software-as-a-service cybersecurity platform and marketplace. Accordingly, this perspective is informed by CrowdStrike's role in protecting organizations from data breaches and a variety of other cyber threats.

II. COMMENTS

CrowdStrike commented on the Australian Government's Discussion Paper on its 2023-2030 Cyber Security Strategy[1] and welcomes the opportunity to comment on this Consultation Paper. The Department of Home Affairs has raised a series of thoughtful questions to consider as it considers legislation to implement Australia's Cyber Security Strategy for 2023-2030. CrowdStrike applauds Australia's goal to become one of the world's most cyber secure countries by 2030, and stands ready to support the Ministry of Home Affairs and its Expert Advisory Board in this journey. While we do not have feedback on every question raised in the Consultation Paper, we do want to offer several points that may be of value to the Australian Government as it develops legislation to implement Australia's Cyber Security Strategy for 2023-2030.

[1] *Request for Comment Response*, *2023-2030 Australian Cyber Security Strategy Discussion Paper*, CrowdStrike, April 2023.
https://www.crowdstrike.com/wp-content/uploads/2023/06/AUS-2023-2030-Cyber-Security-Strategy-Discussion-Paper-Comments.pdf

Measure 1: Helping prevent cyber incidents – Secure-by-design standards for Internet of Things ("IoT") devices

CrowdStrike views secure by design and default principles as a positive initiative to better protect users and drive greater accountability for product makers on security. There are steps that the Australian government can take to incentivize secure by design IoT products, as we note below. While these pertain specifically to network and cybersecurity, they are critical to IoT security as well since security at the network level is a key part of holistic security. In addition, they apply to any type of software used in IoT devices.

Regarding software security, we encourage alignment with CISA's "Secure by Design" principles[2] as well as the updated white paper on the issue, "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software,"[3] that includes expanded principles, guidance, and eight new international agency co-sealers. The scope of this issue can be demonstrated by the international collaboration on this document which includes 17 international partners, including the Australian Signals Directorate[4], all urging software manufacturers to take steps to design, develop, and deliver products that are secure from the very beginning of the process.

As we've previously noted in policy engagement on IoT security, two often overlooked aspects of IoT security involve broader supply chain security protections and protections for IoT application and/or backend infrastructure. With respect to supply chain security, in addition to ensuring secure coding practices and adequate code review, organizations must protect their development platforms and code repositories at least as well as their enterprise environment. In practice, this means that beyond the other security concepts like threat hunting, endpoint detection and response (EDR) technologies aided by AI/ML, organizations must incorporate secure implementation

[2] *Secure-by-Design*, CISA, https://www.cisa.gov/securebydesign

[3] *Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software*, CISA, October 2023. https://www.cisa.gov/sites/default/files/2023-10/Shifting-the-Balance-of-Cybersecurity-Risk-Principles-and-Approaches-for-Secure-by-Design-Software.pdf

[4] The Australian Signals Directorate's document "*IoT Secure-by-Design Guidelines for Manufacturers*", helps manufacturers implement the 13 secure-by-design principles from AS ETSI EN 303 645 standard on cybersecurity for consumer IoT devices. https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-hardening/iot-secure-design-guidance-manufacturers

of both hardware and software, conduct architecture reviews, deploy code signing via tamper resistant hardware, engage in ongoing monitoring, and regular testing.[5]

With respect to support infrastructure, cloud backends may be among the most attractive parts of IoT attack surface to certain types of threat actors. Therefore, cloud security posture is a particularly relevant area of focus.[6] Further, it is increasingly important to focus on application security broadly, and applications are a particularly attractive attack surface in the IoT space.[7]

Measure 2: Further Understanding Cyber Incidents - Ransomware reporting for businesses

Ransomware is still a growing trend. As CrowdStrike's 2024 *Global Threat Report* assesses, ransomware will highly likely remain the primary extortion method through 2024. The report also notes that while ransomware remains the tool of choice for many *big game hunting* (BGH) adversaries, data-theft extortion also continues to be an attractive — and often easier — monetization route. The two can also be deployed together; in fact, since 2019, BGH adversaries have threatened to publish stolen data on dedicated leak sites as a secondary extortion means in concert with deploying ransomware. CrowdStrike assesses that BGH adversaries will increasingly emphasize stolen-data exploitation as a means to pressure victims into payment.[8]

[5] *Request for Comment Response, NIST Cybersecurity Labeling Programs for Consumers: Internet of Things (IoT) Devices and Software*, CrowdStrike, August 17, 2021.
https://www.crowdstrike.com/wp-content/uploads/2021/10/2021-08-17-nist-consumer-software-labeling.pdf

[6] Ibid.

[7] We view application security ("AppSec") as the practice of protecting and securing applications throughout the software development life cycle. AppSec is becoming one of the most essential forms of security for modern enterprises to invest in due to the increased reliance on software. The attack surface is shifting to application and APIs from classic infrastructure configuration and permissions. In fact, eight out of the top 10 data breaches of 2023 were related to application attack surfaces. Today's application security commonly lacks the automation and efficiency needed to support modern applications and the teams that protect them. However, to continuously stay ahead of the adversary, application security posture management and cloud-native application protection platform solutions can be critical. Known vulnerabilities and exploitable code are constantly changing and multiplying; consequently, these potential weakness points should be monitored and analyzed, in real time, for detection, response, and patching purposes.
CrowdStrike State of Application Security Report, CrowdStrike.
https://www.crowdstrike.com/2024-state-of-application-security-report/

[8] 2024 *Global Threat Report*, CrowdStrike, https://www.crowdstrike.com/global-threat-report/

Ransomware reporting requirements, like other information security reporting requirements,[9] involve complex policy equities. To the extent the Government of Australia seeks to advance additional requirements to this end, we encourage: 1) reasonable expectations for small and medium sized enterprises, which are often poorly-resourced, and 2) alignment with requirements in other leading economies to reduce complex or redundant reporting requirements for international entities.

Measure 4: Learning Lessons after Cyber Incidents - A Cyber Incident Review Board

The Consultation Paper seeks input on establishing a Cyber Incident Review Board (CIRB) to conduct no-fault incident reviews and share lessons learned to improve Australia's national cyber resilience. The cybersecurity community benefits from clarity around significant incidents where possible and appropriate, so consideration of a CIRB-like mechanism is timely.

From our perspective, for CIRB to work optimally and achieve its intended objectives, it must:

- Implement clear and transparent governance protocols covering membership; conflict of interest; incident selection criteria; information handling and protection guidelines; and overall incident inquiry scope.
- Not duplicate reviews readily performed by other entities, to include those within the private sector.
- Not duplicate reviews handled competently by other Review Boards, such as the U.S. Department of Homeland Security's Cyber Safety Review Board. For example, CIRB could focus on major breaches of Australian entities; incidents that disproportionately impact Australian citizens; incidents that impact other nations in the region; or in coordination with other Review Board leadership, incidents that the CIRB possesses unique insights or potential to attain clear answers. CIRB could attempt to establish review reciprocity with other Review Boards for incidents that impact multiple nations or their citizens.

[9] *Request for Information Response, Cyber Incident Reporting for Critical Infrastructure Act of 2022*, CrowdStrike, November 14, 2022. https://www.crowdstrike.com/wp-content/uploads/2023/02/RFI-Incident-Reporting-for-Critical-Infrastructure-Act-of-2022.pdf; *Request for Comment Response, FCC Data Breach Reporting Requirements*, CrowdStrike, February 22, 2023. https://www.crowdstrike.com/wp-content/uploads/2023/04/FCC-Data-Breach-Reporting.pdf

III. CONCLUSION

The Consultation Paper raises thoughtful questions around complex and constantly evolving policy areas. As these efforts move forward, we recommend continued engagement with stakeholders. Finally, because the underlying technologies evolve faster than law and policy, we recommend that the strategy focus on principles rather than prescriptive requirements and include a mechanism for periodic revisions.

IV. ABOUT CROWDSTRIKE

CrowdStrike®, a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale AI and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 3 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike: We stop breaches. Learn more: https://www.crowdstrike.com/.

CONTACT

We would welcome the opportunity to discuss these matters in more detail. Public policy inquiries should be made to:

Drew Bagley CIPP/E	**Karen Kaya**
VP & Counsel, Privacy and Cyber Policy	Senior Manager, Public Policy

Email: [redacted]

***