REQUEST FOR COMMENT RESPONSE

2023-2030 AUSTRALIAN CYBER SECURITY STRATEGY DISCUSSION PAPER

April 15, 2023

I. INTRODUCTION

In response to the Australian Government's Minister of Home Affairs Expert Advisory Board's request for comments on the 2023-2030 Australian Cyber Security Strategy Discussion 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

The Expert Advisory Board has raised a series of thoughtful questions to consider as it develops Australia's Cyber Security Strategy for 2023-2030. CrowdStrike applauds Australia's goal to become the world's most cyber secure country by 2030, and stands ready to support the Minister of Home Affairs and its Expert Advisory Board in this journey. We are aware that this effort is being conducted in parallel with the Australia Privacy Act Review, which we commented on separately[1] and encourage alignment with. CrowdStrike provided comments to Home Affairs in 2021[2] and welcomes the opportunity to do so again. While we do not have feedback

[1] *See CrowdStrike Comment on "Privacy Act Review Report 2022,"* March 31, 2023. https://www.crowdstrike.com/wp-content/uploads/2023/04/AUS-Privacy-Act-Review-Comments.pdf

[2] *See CrowdStrike Comment on "Strengthening Australia's Cyber Regulations and Incentives"*, August 27, 2021. https://www.crowdstrike.com/wp-content/uploads/2021/10/2021-08-27-aus-cyber-regs-incentives.pdf

on every question raised in the Discussion Paper, we do want to offer several points that may be of value to the Advisory Board as it develops Australia's Cyber Security Strategy for 2023-2030.

1. What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?

We encourage the Expert Advisory Board to examine the recently-released U.S. National Cybersecurity Strategy[3]. One of the key themes that Australia can take away from that strategy is the need to rebalance the responsibility to defend cyberspace, requiring products to be "secure by design". We suggest it is time that Australia too, requires manufacturers to make products that are "secure by design." As the U.S. strategy points out, the burden to protect society shouldn't be on individuals, small businesses, or local governments, who cannot be required to be society's first line of defense against cyber risks. This burden should be on the manufacturers. The status quo, where new vulnerabilities are discovered in the products of legacy software providers each week, is inadequate.

Furthermore, for Australia to achieve its goal of having its citizens use products with advanced cyber security built-in by-design, and sold at reasonable prices by 2030, the Government should acknowledge that this may mean its citizens use products that come from outside Australia, to leverage the best technology in the world. This also requires allowing the free flow of data across borders. Therefore, we encourage Australia to promote bilateral, multilateral and international agreements that enable the free flow of data across borders, which is especially important for cybersecurity.

2. What legislative or regulatory reforms should the Government pursue to enhance cyber resilience across the digital economy?

d. Should Australia consider a Cyber Security Act, and what should this include?

[3] *See National Cyber Security Strategy*, The White House, March 2023. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

As the Government considers reforms to enhance cyber resilience across the digital economy, or developing a Cyber Security Act, CrowdStrike recommends the consideration of the following principles and technologies as a baseline. We view these as best practices for a comprehensive, risk-based, cybersecurity strategy.

- **Extended Detection & Response (XDR).** Cybersecurity threats are exceptionally broad, and for too long industry players have focused on narrow solutions. No box on a network or a single-purpose software agent will address the full scope of the problem. Security teams demand contextual awareness and visibility from across their entire environments, including within cloud and ephemeral environments. The next evolution of the ***Endpoint Detection and Response* (EDR)** concept, XDR seeks to leverage rich endpoint telemetry and integrate other security-relevant network or system events, wherever they exist within the enterprise, and generate intelligence from what otherwise may be an information overload. EDR is a great place for organizations to start with baseline security; however, XDR is an option for organizations with already advanced cybersecurity practices.

- **Identity Protection and Authentication**: As organizations embark on a digital transformation to work from anywhere models, Bring-Your-Own-Device policies become commonplace, cloud services multiply, and enterprise boundaries continue to erode. This trend increases the risk of relying upon traditional authentication methods and further weakens obsolescent legacy security technologies. Identity-centric approaches to security use a combination of real-time authentication traffic analysis and machine learning analytics to quickly determine and respond to identity-based attacks.

- **Logging Practices**. Organizations should collect and retain security-relevant log information to support proactive security measures, threat hunting, and investigative use-cases.

- **Threat Hunting**. Whether through supply chain attacks or otherwise, we know that adversaries periodically breach even very-well defended enterprises. Properly trained and resourced defenders can find them and thwart their goals. In our experience, whether organizations accept this

premise – that cybersecurity involves not just a passive alarm, but a sentry actively looking for trouble – is the leading indicator of the strength of their cybersecurity program. Central to hunting is properly instrumenting enterprises to support both automated and hypothesis-driven adversary detection. And the better-instrumented the environment, the more chances defenders give themselves to intervene as a breach attempt progresses through phases, commonly referred to as the *kill chain*. Multiple opportunities for detection help avert "silent failures" – where a failure of security technology results in security events going completely unnoticed.

- **Speed**. We advise users that when responding to a security incident or event, every second counts. The more we can do to detect and stop adversaries at the outset of an attack, the better chance we have to prevent them from achieving their objectives. The reason for this is that adversaries move fast, especially when engaging in lateral movement through an enterprise. This means that measuring response time and severity, essentially a DEFCON for security, is critical to ultimately stopping a malicious chain of events and improving performance.

- **Machine Learning-Based Prevention**. The core of next-generation cybersecurity solutions is the ability to defeat novel threats. Machine learning and artificial intelligence are essential to this end, and leveraging these technologies is the best way to gain the initiative against adversaries.

- **Zero Trust.** Due to fundamental problems with today's widely-used authentication architectures, organizations must incorporate new security protections focused on authentication. Zero Trust design concepts radically reduce or prevent lateral movement and privilege escalation during a compromise.

- **Consideration of Managed Service Providers**. Some entities lack the cybersecurity maturity to run effective security programs internally. Increasingly, such entities should rely upon managed service providers to achieve a reasonable level of security. These programs scale easily and are an increasingly affordable way for companies to achieve cybersecurity coverage

24 hours a day, 7 days a week, 365 days a year.

- **Cloud Security**. There are multiple benefits to deprecating legacy, on premises systems and leveraging cloud systems. These include operational efficiencies, enhanced visibility and security, and contracting efficiencies.

4. What opportunities exist for Australia to elevate its existing international bilateral and multilateral partnerships from a cyber security perspective?

We applaud Australia's leadership in the International Counter Ransomware Task Force as the inaugural chair and Secretary Pezzullo spearheading an incident response workstream for the Task Force. One of the outcomes of that summit was a commitment to actively share information between the public and private sectors, on actors and tradecraft. Australia can use this as an opportunity to facilitate and encourage further international and private-public cooperation. Australia's position in the Quadrilateral Security Dialogue (QUAD) is another opportunity to elevate its existing international partnerships in cyber security, as is the Indo-Pacific Economic Framework for Prosperity (IPEF).

5. How should Australia better contribute to international standards-setting processes in relation to cyber security, and shape laws, norms and standards that uphold responsible state behaviour in cyber space?

Australia should work closely with like-minded nations in international standard-setting bodies such as the International Telecommunications Union (ITU) to ensure that the principles adopted in the 'Declaration for the Future of the Internet" are upheld globally. We need to ensure that like-minded nations like us continue to lead on global rules and values, by our example. To achieve this, we encourage Australia to adopt a message that frames all policies in affirmative, positive and compelling terms, telling a real story about the good things that tech can bring to our future, with a view to encourage middle-states in the world to align with us.

6. How can Commonwealth Government departments and agencies better demonstrate and deliver cyber security best practice and serve as a model for other entities?

The Commonwealth Government department and agencies should lean into an enterprise-wide approach, reflective of the paradigm shift that entails moving away from distinct approaches at the city or local levels. This will require enhancing and harmonizing regulatory frameworks; while simplifying and streamlining existing ones. The Government should also explore collaboration between federal, state and territory government agencies. For cyber security best practices and serving as a model for other agencies, please see our response to question 2 above.

Furthermore, as we wrote in our 2021 comment on "Strengthening Australia's cybersecurity regulations and incentives", an often overlooked policy area, even among nations with leading cybersecurity capabilities, is for the government to lead by example in terms of maintaining an exceptionally strong cybersecurity posture. To this end, CrowdStrike recommends Australia's government department and agencies implement the "1-10-60 Rule" or similar metrics. This concept challenges enterprises to detect malicious cyber activity within one minute, have a human investigate that detection within 10 minutes, and remediate or isolate any compromised assets within 60 minutes. This rule serves as an organizing principle for security personnel training and staffing, technology acquisitions and modernization projects. This recommendation represents an ambitious program that only organizations with mature security programs can achieve. But measuring these metrics, testing security programs against them and tracking performance over time can be remarkably effective.

Comprehensive visibility across the enterprise is the first step to strengthening security posture. The CrowdStrike Falcon® platform operates on this basis, enabled by a massive distributed graph database using cloud-scale AI and deep link analysis to identify threats. This means threats targeting disparate entities and organizations can be identified and prevented. As soon as a malicious indicator or behavior is identified anywhere, it can be stopped everywhere.

A few additional practices will help on this journey. Governments should use shared-services acquisition models where possible. These models drive

procurement efficiencies by reducing the number of contracting actions required to support multiple departments and agencies. They also provide simpler training requirements, easier management and maintenance, and reduced administrative complexity. From an operational perspective, they enable standardized service levels across government — and even more importantly — a common operating picture across federated entities.

7. What can the government do to improve information sharing with industry on cyber threats?

Regarding the government sharing information with industry on cyber threats, we encourage the Expert Advisory Board to examine the U.S. Joint Cyber Defense Collaborative (JCDC) platform. Established in 2021, the JCDC is a good example of how the public and private sector share information and drive collective action across the cybersecurity community in the U.S. It is somewhat similar to Australia's Cyber Threat Intelligence Sharing (CTIS) Program, which establishes a national community of organizations that share threat intelligence bilaterally. Participating organizations in the JCDC include federal and state government agencies and private sector organizations across multiple industry sectors. It is a platform where vendors can aggregate or intermediate information, making it useful for JCDC to involve key industry stakeholders rather than attempt to integrate every single individual company. Vendors also have key insights, capacities, and interests in sharing and planning. The JCDC's goal is to bring together the right sets of partners to address the right specific risks, regardless of whether they are urgent or long-term. Similarly, when there's a new major vulnerability, the JCDC's goal is to bring in the right sets of partners to counter it. The ultimate goal is to have every organization participating in the JCDC, or having a relationship with it, as well as an agreement that governs how the information shared with it will be secured.

We hope organizations like JCDC or Australia's CTIS program, as well as international collaborations such as the International Counter Ransomware Task Force, expand into "operations"; particularly proactive operations where the vendor community is collaborating with international like-minded partners to disrupt adversary infrastructure.

10. What best practice models are available for automated threat-blocking at scale?

Next-generation solutions, which leverage AI/ML, can detect previously unknown threats based on their characteristics or behaviors at scale. This offers much more robust protection against threat activity. Leveraging AI/ML can achieve success against unknown unknowns. For example, a machine learning model, shipped to CrowdStrike's Falcon Platform customers in September 2019, detected with high confidence the SUNSPOT malware, which was central to a sophisticated campaign that targeted high-value government organizations in late 2020-early 2021.[4] This is one of many instances of AI/ML typifying the best ways to defeat threat actors using new or tailored tools, tactics, techniques, or procedures.

In cybersecurity, AI is an advantage, especially when added to enterprise security solutions.[5] Cybersecurity threats are exceptionally broad, and for too long industry players have focused on narrow solutions. No box on a network or a single-purpose software agent will address the full scope of the problem. Security teams demand contextual awareness and visibility from across their entire environments. Indeed, with the help of AI, CrowdStrike can stop an attack in its tracks because such technology works faster than conventional signature-based or indicator of compromise (IOC)-based prevention.

13. How should the government respond to major cyber incidents (beyond existing law enforcement and operational responses) to protect Australians?

a. Should government consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators?

---

[4] *See Sven Krasser, "Stellar Performances: How CrowdStrike Machine Learning Handles the SUNSPOT Malware,"* CrowdStrike Blog, Jan. 21, 2021 https://www.crowdstrike.com/blog/stellar-performances-how-crowdstrike-machine-learning-handles-the-s unspot-malware/.

[5] *See Michael Sentonas, How Artificial Intelligence is Becoming a Key Weapon in the Cybersecurity War*, CrowdStrike Blog, Oct. 24, 2017, https://www.crowdstrike.com/blog/how-artificial-intelligence-is-becoming-a-key-weapon-in-the-cybersecu rity-war/.

CrowdStrike views the establishment of a Coordinator for Cybersecurity as well as a National Office for Cyber Security within Home Affairs as a positive first step towards taking a harmonized approach to cyber security. As a next step, CrowdStrike recommends the government consider a single reporting portal for all cyber incidents, harmonizing existing requirements to report separately to multiple regulators. The Coordinator for Cybersecurity, working with the National Office for Cyber Security, should develop a draft of the data fields to be asked in the reporting mechanism and a workflow of the submission procedures. We recommend that they then release a draft version of the data fields and forms to industry for another round of stakeholder engagement – whether that be through a Request for Comment period or workshops. Without proposed data fields or a draft template to respond to, it is difficult for organizations to envision the types of information that is most useful to the Coordinator for Cybersecurity.

Once the report contents are resolved, to the extent possible, the Coordinator should make available a variety of reporting formats to fit the needs of different entities. While certain information should be mandatory to report, as determined through the stakeholder engagement efforts, digital report formats can allow the Coordinator to gather additional fields of information. The Coordinator should explore creating workflows that would allow victim organizations to explicitly be permitted to refer reports to other regulators to streamline other reporting requirements or obligations.

19. How should the Strategy evolve to address the cyber security of emerging technologies and promote security by design in new technologies?

On this question too, we encourage looking at the U.S National Cyber Security Strategy, which calls for re-aligning incentives to design new technologies that are "secure by design". The document calls for incentives that favor long-term investments for secure products, rather than short and quick fixes focused on getting a product out to market quickly.

III. CONCLUSION

The Expert Advisory Board's Discussion Paper raises thoughtful questions on its journey to develop Australia's Cyber Security Strategy for 2023-2030. As updates to

the law and administrative rulemaking moves forward, we recommend continued engagement with stakeholders. Finally, because the underlying technologies evolve faster than law and policy, we recommend and emphasize that any legislative updates and proposed rulemaking focus on principles rather than prescriptive requirements and include a mechanism for periodic revisions.

IV. ABOUT CROWDSTRIKE

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with one of the world's most advanced cloud-native platforms for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

Learn more: https://www.crowdstrike.com/

V. CONTACT

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

Drew Bagley CIPP/E
VP & Counsel, Privacy and Cyber Policy

Fabio Fratucello
Field CTO, International

Email: policy@crowdstrike.com

***