REQUEST FOR COMMENT RESPONSE

Strengthening Australia's cybersecurity regulations and incentives

27 August 2021

I. INTRODUCTION

In response to the Department of Home Affairs' request for public consultation on strengthening Australia's cybersecurity regulations and incentives, 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, 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

A. Cybersecurity Standards: Setting Clear Expectations

To reach the goal of setting clear expectations, as well as defending a complex enterprise, CrowdStrike recommends a uniform, high-level standard of cybersecurity. Separate standards will result in unintended short-term and long-term consequences. In the short term, different rules and standards will yield divergent results, complicate security training, negatively impact the use of shared resources and services, and complicate collaboration between organizations and agencies. In the long term, independently-developed approaches will lead to confusion with respect to emerging security controls and updates to best practices. Consequently, this increases the risk of cybersecurity incidents.

More broadly, the adoption of principles-based cybersecurity requirements can incentivize both innovation and organizational implementation of state-of-the-art technologies to protect data. While the Notifiable Data Breaches scheme is already influencing organizations to treat security breaches seriously, there are additional steps that can encourage proactive adoption of cutting-edge technologies, such as software-as-a-service (SaaS) solutions, from around the globe. The European Union General Data Protection

Regulation (GDPR), for example, requires organizations to look to the "state of the art" and protect personal data with technological and organizational safeguards "appropriate to the risk." Creating non-prescriptive mandates that nonetheless encourage organizations to analyze the probability and severity of threats in line with technological realities is important for ensuring cybersecurity evolves with critical technologies.

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 governments implement the "1-10-60 Rule" or similar metrics.[1] 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.

B. Increasing Transparency and Disclosure

[1] This concept is also relevant to the private sector. Most recently, the U.S. Cyberspace Solarium Commission recommended that the U.S. Congress require public companies to track cyber incident time to detection, time to investigation, and time to remediation metrics in order to continuously improve defenses. *See* U.S. Cyberspace Solarium Commission, *Final Report*. March 2020. p. 83. https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view.

1. Labelling for smart devices

Several markets are exploring labeling schemes for smart devices, such as commercial Internet of Things ("IoT") devices. These devices are composed of a variety of embedded software, sensors, and other technologies. Unclear information regarding these components and attributes, as well as uneven security properties, complicate consumers' efforts to make informed decisions about purchases, use cases, and risk mitigations.

Requiring industry to provide information to consumers, such as whether an IoT device can leverage third-party security technologies, will incentivize industry to make more securable IoT devices, as well as enable users to make the best decision for their needs. This may not be necessary for most consumer use cases, but consumer-grade smart devices are frequently utilized by enterprises, and in those cases the ability to leverage best practice technologies like Extended Detection and Response (XDR) will play a critical role in identifying and preventing threats.[2]

The future of IoT and other devices is so robust that it is worth designing schemes to address these issues. Such schemes should be straightforward to comply with and easy to use; they should be designed collaboratively with a broad cross-section of stakeholders, including manufacturers and security providers; and should include provisions for updating the scheme as technology evolves and threats change.

2. Health Checks for Small Businesses

Regarding the proposed health checks on small businesses, it is important to emphasize that today, the failure of a business of any size, from a startup to a tech giant, to meet data protection obligations may pose a risk to the privacy of individuals. Consequently, it is paramount that businesses have access to the tools they need to protect the data of their customers without overburdening owners and operators. The proposed health checks are a tool to help a business protect data and increase understanding about the importance of cybersecurity.

Participation in health checks may increase compliance obligations in the short term, but it may help those businesses avoid a detrimental consequence later. Even a single data breach

---

[2] *See generally* IT Security Act (Germany) and EU General Data Protection Regulation: Guideline "State of the Art" Technical and Organizational Measures, Teletrust (2021), https://www.teletrust.de/fileadmin/user_upload/2021-02_TeleTrusT-Guideline_State_of_the_art_in_IT_security_EN.pdf; George Kurtz, Testimony on Cybersecurity and Supply Chain Threats, Senate Select Committee on Intelligence (Feb. 23, 2021), https://www.intelligence.senate.gov/hearings/open-hearing-hearing-hack-us-networks-foreign-adversary.

can have a devastating impact on a small business, which may be difficult to recover from. The adoption of a collaboratively-designed small business health check trust mark could be of benefit, as small businesses may use it from a marketing perspective, increasing consumer confidence in their offerings.

III. CONCLUSION

The Department of Home Affairs proposal provides a thoughtful analysis of a complex legal and policy area. As the Department updates its regulations, we recommend continued engagement with international stakeholders. Adversaries innovate at a record-pace, and it's important to empower defenders to leverage global data flows, big data analytics, and machine learning to protect against ever-evolving threats. Finally, because the underlying technologies evolve faster than law and policy, we recommend and emphasize that any proposed legislative updates focus on principles rather than prescriptive requirements and include a mechanism for periodic revisions.

IV. ABOUT CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq: CRWD), 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/.

V. CONTACT

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

Michael Sentonas **Drew Bagley CIPP/E**

Chief Technology Officer VP & Counsel, Privacy and Cyber Policy

Email: policy@crowdstrike.com

***