REQUEST FOR COMMENT ON CCPA UPDATES, CYBER, RISK, ADMT, AND INSURANCE REGULATIONS

February 19, 2025

I. INTRODUCTION

In response to California Privacy Protection Agency's (CPPA) proposed updates to CCPA Cyber, Risk, ADMT, and Insurance regulations (proposed regulation) 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 appreciates the CPPA's continued engagement with stakeholders and the opportunity to provide comments on the proposed regulation. We continue to support the proposed regulation's goal of better protecting California's businesses and citizens from cybersecurity threats. Incentivizing the adoption of effective cybersecurity practices and technologies is paramount to achieving the CPPA's goal of protecting citizen's data.

CrowdStrike previously commented on the initial version of the proposed regulation, and we've reemphasized certain points in this response.[1] We do not have feedback on every aspect of the proposed regulation, but we do want to offer several points that may be of value to the CPPA.

A. Cybersecurity Audits

[1] *Invitation for Preliminary Comments on Proposed Rulemaking*, CrowdStrike, March 27, 2023. https://www.crowdstrike.com/wp-content/uploads/2023/04/CPPA-Cybersecurity-Comments.pdf

Audits have significant limitations in driving cybersecurity outcomes. They are a useful tool for an organization to capture a snapshot of the existence of cybersecurity plans, strategies, or controls. But ultimately audit results are only reflective of a point in time and cannot reflect a real-time measure of the state of an organization's security posture. With this in mind, we would caution organizations against being overly reliant on the results.

However, the practices and tools the CPPA has outlined for organizations to check for in an audit do represent many of today's cybersecurity best practices. Having, and maintaining day-to-day, these practices can help organizations continuously protect themselves from cyberattacks and data breaches. In addition to following cybersecurity best practices, organizations must reevaluate if those technologies are working to the best of their ability more regularly than a yearly audit. Below are a few cybersecurity best practices included in the audit requirements.

a. Identity Protection

We welcome the inclusion of identity protection in the proposed regulation. The CPPA includes components such as authentication, account management and access controls, and monitoring. This is important because effective identity protection requires a holistic view. Relying upon traditional authentication methods is no longer enough to protect organizations from cyberattacks. Identity-centric approaches to security use a combination of real-time authentication traffic analysis and machine learning analytics to quickly identify and respond to identity-based attacks. Given that the audit components are flexible, organizations undergoing this internal exercise should consider additional steps in their identity protection scheme beyond the basics outlined in the regulation.

b. Zero Trust Architecture

As noted by the CPPA, closely related to identity protection is Zero Trust Architecture (ZTA), which eliminates transitive trust and radically reduces and prevents lateral movement and privilege escalation during a compromise. This constrains threat actors' ability to achieve actions on objective and provides additional opportunities for defenders to detect threats. ZTA is an important adjunct to multifactor authentication (MFA)-based guidance, and other baseline identity measures, because it can stop attacks even if legitimate credentials are compromised and MFA is bypassed. Therefore, it is a constructive element of the proposed regulation.

c. Logging Practices

The CPPA accurately notes that organizations should collect and retain security-relevant log information to support proactive security measures, threat hunting, and investigative use-cases. Indeed, where utilized, Next Generation Security Information and Event Management (Next-gen SIEM) solutions leverage such data to drive better security outcomes.

d. Threat Hunting

Finally, whether through supply chain attacks or otherwise, adversaries periodically breach even very-well defended enterprises. However, skilled defenders can find them and thwart their goals. Proactive threat hunting is a leading indicator of the strength of an enterprise cybersecurity program. Central to threat hunting is properly instrumenting enterprises to support both automated and hypothesis-driven adversary detection. The more well-instrumented the environment, the more opportunities defenders give themselves to identify malicious activity as an attack progresses through phases. Optimally defenders or their service providers continually hunt for threat activity 24/7, 365 days per year. Threat hunting is closely related to the network monitoring and defense, and cybersecurity threat awareness components in the regulation - likely, an organization that is completing those components well would have threat hunting as part of their process.

e. Endpoint Detection and Response

Relatedly, endpoint detection and response (EDR) solutions are a necessary part of a cybersecurity strategy to protect organizations from threats. EDR defends endpoints such as desktops, laptops, servers, mobile devices, cloud workloads, and from malicious activity, and provides granular visibility of potential threats. This enables holistic, real-time threat detection and proactive threat prevention. Leveraging EDR, defenders can perform threat hunting, incident response, and a variety of other essential cybersecurity tasks. If an organization deploys the other components in the audit regulation, an organization likely would have, or need to have, EDR solutions as part of their cybersecurity strategy. For these reasons, adding a component that addresses uses and implementation of EDR solutions would strengthen the proposed regulation.

B. Risk Assessments

Risk assessments are distinct from audits and should not be standards-driven. The fundamental question of a risk assessment is "how effectively does the security program address the cyber risks the organization faces?" Flexible frameworks are ideal for this type of evaluation as risk assessments need to be tailored for the organization completing it. The best risk assessments should combine the types of security measures but place them in an operational context - both in terms of what threat actors are likely to exploit and what defenders can realistically accomplish.

Risk assessments are an internal exercise, often done under client privilege with a third-party firm, and businesses should not be required to submit risk assessments to the CPPA. If organizations are required to submit risk assessments to an agency - even an abridged version – it could move the assessment from a thoughtful exercise to purely a checklist compliance measure. A risk assessment that is shared with an agency might also discourage or deter organizations from fully investigating problems, or digging deeper if an issue is spotted, in fear of repercussions once the assessment has been shared externally.

Finally, the risk assessment section should mirror the Automated Decisionmaking technology section (addressed further below) and add an exception for risk assessments for use of personal data for security, fraud prevention, and safety purposes.[2] State-of-the-art cybersecurity practices require processing many categories of data, and at a minimum personal information is often necessary for a cybersecurity provider to alert customers to threats.

C. Automated Decisionmaking

CrowdStrike applauds the CPPA including a security carveout into the regulations for automated decisionmaking technologies. The use of Artificial Intelligence (AI) to detect cyber threats is an enormous advantage. Today, security teams demand contextual awareness and visibility from across their entire environments, including within cloud and ephemeral environments, and AI can help defenders process this data and make detections more actionable. AI is the best tool defenders have to identify and prevent zero-day attacks and malware-free attacks, because AI can defeat novel threats based on behavior cues rather than known signatures. Leveraging these technologies is essential to meeting constantly-evolving threats. If individuals were able to opt-out of

[2] CPRA Proposed Text of Regulations § 7221(1)

AI uses for cybersecurity, it could allow adversaries to conduct harm undetected.

III. CONCLUSION

The CPPA's proposed rulemaking represents a thoughtful attempt to strengthen security outcomes in a complex legal and policy environment. As the CPPA 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 proposed legislative updates 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

Elizabeth Guillot
Senior Manager, Public Policy

Email: policy@crowdstrike.com

***