CROWDSTRIKE

INVITATION FOR PRELIMINARY COMMENTS ON PROPOSED RULEMAKING

CYBERSECURITY AUDITS, RISK ASSESSMENTS, AND AUTOMATED DECISION MAKING

March 27, 2023

I. INTRODUCTION

In response to the California Privacy Protection Agency's ("CPPA") invitation for preliminary comments on proposed rulemaking regarding cybersecurity audits, risk assessments, and automated decision making ("proposed rulemaking") 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

We appreciate the CPPA's efforts to better protect California citizens' data from cybersecurity threats through the California Privacy Rights Act of 2020 ("CPRA"). Although CrowdStrike submitted a response to the November 2021 invitation for preliminary comments on these same issues, we welcome the opportunity to provide additional feedback.[1]

Cybersecurity threats are evolving and increasing. Illustrative of this, in CrowdStrike's 2023 *Global Threat Report*, we observed a notable surge in identity-based threats and cloud exploitations. To name a few, we found a 112%

[1] CrowdStrike's response to the Invitation for Preliminary Comments on Proposed Rulemaking, pages 17-23: https://cppa.ca.gov/regulations/pdf/preliminary_rulemaking_comments_1.pdf

year-over-year increase in advertisements on the dark web for identity and access credentials, a 95% increase in cloud exploitation by threat actors, over 30 new adversaries and numerous new ways that eCrime actors weaponize and exploit vulnerabilities.[2] As adversaries continue to evolve and find new ways to target victims, organizations need to increase their emphasis on cybersecurity practices that leverage the most effective technologies.

The legal and regulatory environment surrounding cybersecurity is increasingly complex. This follows from: (i) growing reliance on globally-distributed infrastructure, and (ii) compliance obligations for national and international standards and procedures. In order to ensure the most robust cybersecurity methods and disclosure, and compliance obligations remain feasible, regulators must endeavor to create clear and future-flexible expectations.

While we do not have feedback on every aspect of the proposed amendment, we do want to offer several points that may be of value to the CPPA as it considers the proposed rule.

A. Cybersecurity Audits

Cybersecurity audits have significant limitations as a cybersecurity tool. They are a useful tool for an organization to capture a snapshot of the existence of cybersecurity plans, strategies, or controls; however, 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 practices. While we recognize that it is the CPPA's intention to create an auditing scheme, we would caution organizations against being overly reliant on the results. In addition to a cybersecurity audit, organizations should deploy cybersecurity best practices to continuously protect themselves from cyberattacks and data breaches and reevaluate if those technologies are working to the best of their ability more regularly than a yearly audit. Creating non-prescriptive mandates that nonetheless encourage organizations to analyze their risks, plans, and strategies is important for ensuring cybersecurity practices evolve with the threat landscape.

Incentivizing the adoption of effective cybersecurity practices and technologies is

[2] *CrowdStrike Global Threat Report, 2023. https://www.crowdstrike.com/global-threat-report/*

paramount to achieving the CPPA's goal of protecting citizen's data. CrowdStrike views the following strategies and technologies as best practices and recommends the best practices be deployed by entities in scope of the regulations.

- **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.

As the CPPA is creating audit metrics, the Agency should align with existing, widely adopted standards and guidelines. Splintering standards, across states and the federal government, 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.

As such, cybersecurity audits should test compliance against established standards recognized by the Agency as most appropriate, whether that be NIST, ISO, or other widely-used and adopted standards. Currently, NIST is in the process of updating their Cybersecurity Framework. We recommend that the CPPA closely review the final version of the Cybersecurity Framework 2.0 and consider it as a framework organizations can follow during an audit.

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. Instead, the CPPA should provide a resource of a draft risk assessment to organizations in scope to help them undertake the assignment internally. If organizations were required to submit risk assessments to an agency, 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.

C. Automated Decisionmaking

From CrowdStrike's perspective, the proposed rulemaking is solely focused on consumers facing automated decisionmaking. CrowdStrike agrees with keeping the focus of the proposed rulemaking on consumer-facing automated decisionmaking or artificial intelligence (AI). In enterprise (B2B) technologies that use AI, a contract has been created and agreed to by both parties which includes privacy protections for individuals that are a part of the businesses entering into the contracts. This is different from consumer facing AI where there is not an agreement in place between the AI technology and every consumer that may come in contact with the technology.

CrowdStrike recommends adding a security carveout into the regulations for all business purposes. This would be in alignment with the exception under section 7050(a)(4) of the Chapter 1 regulations. In cybersecurity, AI is an advantage, especially when added to enterprise security solutions. Cybersecurity threats are exceptionally broad, and for too long industry players have focused on narrow solutions. Security teams demand contextual awareness and visibility from across their entire environments, including within cloud environments. To give an example, 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. Usually these use cases fall under the B2B agreements described above, but to ensure that security companies are able to continue protecting against the same threats the CPRA aims to, a cybersecurity technology exemption to the automated decisionmaking section is needed.

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®, 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	**Elizabeth Guillot**
VP & Counsel, Privacy and Cyber Policy	Manager, Public Policy

Email: policy@crowdstrike.com

marks, and may use the brands of third parties to identify their products and services.

***