REQUEST FOR COMMENT ON PROPOSED SECOND AMENDMENT TO 23 NYCRR Part 500

CYBERSECURITY REQUIREMENTS FOR FINANCIAL SERVICES COMPANIES

January 9, 2023

I. INTRODUCTION

In response to New York's Department of Financial Services ("DFS") Proposed Second Amendment to 23 NYCRR Part 500, Cybersecurity Requirements For Financial Services Companies ("proposed amendment") 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 DFS's efforts to better protect New York's and the nation's financial services sector from cybersecurity threats. Cybersecurity threats are evolving and increasing. Illustrative of this, in CrowdStrike's 2022 *Global Threat Report*, we observed a 82% increase in ransomware-related data leaks (from 2021 - 2022).[1] The financial services sector is included in that figure and also saw a sharp increase in data leaks from ransomware attacks – making steps to enhance cybersecurity in the sector timely and appropriate.

[1] 2022 *Global Threat Report*, CrowdStrike, https://www.crowdstrike.com/global-threat-report/

The legal and regulatory environment surrounding cybersecurity is increasingly complex on account of (i) 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 DFS as it considers the proposed rule.

A. Cybersecurity Risk Management Practices

We commend the DFS for strengthening cybersecurity by amplifying attention given to this issue and defining expectations. There are some key steps organizations should take to strengthen their security posture. The proposed amendment includes many of today's most effective cybersecurity practices. Notably, several of these practices are also mandated in the May 2021 federal Executive Order (EO) 14028 on Improving the Nation's Cybersecurity.[2] CrowdStrike applauds the inclusion of the following technologies and principles in the proposed amendment and recommends they continue to be included in the final amendment.

- **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. The proposed amendment requires EDR, which is a great place to start, however; we

[2] White House, *Executive Order 14028: Improving the Nation's Cybersecurity* (May 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

recommend the language be revised to also include XDR as an option for organizations with 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.

As DFS revises the proposed amendment, CrowdStrike recommends the consideration of the following principles and technologies as requirements for cybersecurity programs. We view the following as best practices for a comprehensive, risk-based, cybersecurity strategy.

- **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.

- **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 the level of security appropriate for listed companies. Organizational transformations along these lines often involve a cross section of departments or teams (*e.g.*, personnel, finance, security, human resources) and can be most expeditiously resolved at the leadership-level.

B. Harmonization

As DFS reviews this proposed amendment, and drafts other pieces of regulation, CrowdStrike urges alignment where possible with existing rules and regulations. We recommend alignment with the Cyber Incident Reporting for Critical Infrastructure Act of 2022 and the forthcoming implementing regulation. Additionally, there will be harmonization recommendations resulting from the ongoing work of the Cyber Incident Reporting Council to align federal cyber incident structures and requirements that should be followed when appropriate by state governments.

CrowdStrike also recommends alignment with industry best practices in the vulnerability space. Within the private sector, longer-term vulnerability disclosure norms have emerged. For example, in general, security researchers make a 90 day allowance following the discovery and reporting of a vulnerability in another

vendor's software.[3] Even when vulnerabilities are being actively exploited, organizations typically have seven or more days before the researcher makes a disclosure. Exacerbating factors where public notice could be detrimental to an ongoing incident response investigation include, for example, when data extortion is at play, a law enforcement investigation mandating confidentiality, or where it may take additional time to incorporate the preventative measures necessary to prevent an even more significant impact (such as in vulnerability disclosure). The proposed amendment's current language would allow organizations to adopt these best practices.

III. CONCLUSION

The DFS's proposed amendment represents a thoughtful attempt to strengthen security outcomes in a complex legal and policy environment. Generally speaking, the financial sector uses strong cybersecurity practices due to the amount of sensitive data they protect and the regulations to which they are subject. With an emphasis on adoption of practical security practices, these new requirements can raise the already high standard of cybersecurity in the financial sector. As the DFS 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.

[3] *See generally*, Tim Willis, *Project Zero* (Apr. 12, 2021), https://googleprojectzero.blogspot.com/2021/04/policy-and-disclosure-2021-edition.html.

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
VP & Counsel, Privacy and Cyber Policy

Robert Sheldon
Director, Public Policy & Strategy

Email: policy@crowdstrike.com

***