REQUEST FOR COMMENT ON REVISED NEW YORK HOSPITAL CYBERSECURITY REQUIREMENTS

June 28, 2024

I. INTRODUCTION

In response to New York's Department of Health ("Department") revised proposed regulation to create cybersecurity requirements for all hospital facilities ("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 Department's continued engagement with stakeholders and the opportunity to provide comments on the updated proposed regulation. We continue to support the proposed regulation's goal of better protecting New York's hospitals and citizens from cybersecurity threats. These threats continue to evolve and grow more severe. In a recent report, we found that 8% of all interactive intrusions – i.e., those with a human at the keyboard, not a bot or spam – in 2023 impacted the healthcare sector.[1] Additionally, healthcare was one of the top sectors advertised by access brokers in 2023, which demonstrates how attractive the sector is to those monetizing breaches.[2]

[1] 2024 *Global Threat Report*, CrowdStrike, https://www.crowdstrike.com/global-threat-report/
[2] 2024 *Global Threat Report*, CrowdStrike, https://www.crowdstrike.com/global-threat-report/

CROWDSTRIKE

CrowdStrike previously commented on the initial version of the proposed regulation, and we've reemphasized certain points in this response.[3] 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 Department.

A. Cybersecurity Risk Management Practices

We commend the Department 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 regulation includes some 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.[4]

CrowdStrike applauds the continued inclusion of managed service providers, or third-party service providers, as a means to assist in complying with the requirements in the regulation. As the Department recognizes, 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 covered organizations.

Additionally, we welcome the inclusion of identity projection in the proposed regulation. The Department's "Identity and Access Management" section in the updated proposed rule takes a holistic view of this priority area. 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 determine and respond to identity-based attacks. In our experience, organizations that do not leverage the latest technologies and frameworks for identity protection are not set up for success against cyberattacks.

The proposed amendment has multi-factor authentication ("MFA") requirements in place. However, MFA is just one piece of an "Identity and Access Management"

[3] *Request for Comment on Proposed Hospital Cybersecurity Requirements*, CrowdStrike, Feb 2, 2023. https://cs-staging-2-www.crowdstrike.com/wp-content/uploads/2024/02/NY-Hospital-Cybersecurity-Comments.pdf.

[4] 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/.

framework hospitals should have in place. Zero trust architecture is an important adjunct to MFA-based guidance because it radically reduces or prevents lateral movement and privilege escalation during a compromise, and can stop attacks even if legitimate credentials are compromised and MFA is bypassed.

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. Organizations with already advanced cybersecurity programs, should further leverage next-generation security information and event management (SIEM) solutions. Next-gen SIEM aggregates telemetry, like that captured by EDR, and integrates it with other security-relevant event information from an array of sources to deliver defenders a cohesive view of their environment. Given that organizations have many connected devices, EDR, as a baseline, is essential to identify and proactively prevent threats. Along with MFA, EDR should be included as a requirement in this regulation.

In addition to zero trust and EDR, in our previous comments, we also suggested the consideration of logging, threat hunting, and machine learning-based prevention. Next-gen SIEM solutions, as described above, enable these priorities. We view these as key elements of a comprehensive, risk-based, cybersecurity strategy. In the assessment of public comments, the Department states, technology products, services, and solutions are outside the scope of the proposed rulemaking; however, the assessment also states that future guidance around current industry best practices for risk assessments is anticipated.

CrowdStrike respects, and agrees with, the concept that different entities require different cybersecurity solutions. However, as stated previously, we view EDR, zero trust, logging, threat hunting, and machine learning-based prevention principles and technologies as best practices within a comprehensive cybersecurity strategy. Rather than release an additional document with industry best practices in the future, the Department should do so within the final version of the proposed regulation.

B. Incident Reporting Timeline

The updated proposed regulation revises the incident reporting timeline to 72 hours. This timeline is emerging as a best practice, both in the U.S. and internationally. We appreciate the Department listening to stakeholder feedback on this issue to bring the regulation into alignment with the emerging standard.

III. CONCLUSION

The Department's proposed regulation represents a thoughtful attempt to strengthen security outcomes in a complex legal and policy environment. Generally speaking, the healthcare 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 healthcare sector. As the Department moves forward, we recommend continued engagement with stakeholders.

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

***