REQUEST FOR COMMENT ON NEW YORK HOSPITAL CYBERSECURITY REQUIREMENTS

February 2, 2024

I. INTRODUCTION

In response to New York's Department of Health ("Department") 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 supports 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, for example, we found that interactive intrusion activity against the healthcare sector increased significantly over the past year.[1] Furthermore, the report found a 147% increase in access broker[2] advertisements on the dark web, a 95% rise in cloud attacks, and a sharp increase in credential theft – making steps to enhance cybersecurity in the sector timely and appropriate.

CrowdStrike appreciates New York's continued efforts to improve cybersecurity across critical sectors. Of note, we previously submitted comments to New York's Department

[1] 2023 *Threat Hunting Report*, CrowdStrike, https://www.crowdstrike.com/resources/reports/threat-hunting-report/.
[2] Access Brokers: Who Are the Targets, and What Are They Worth?, https://www.crowdstrike.com/blog/access-brokers-targets-and-worth/

of Financial Services ("DFS") regarding amendment to the Cybersecurity Requirements for Financial Services.[3]

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

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 that would help accomplish the proposed regulation's directive of building a cybersecurity program that identifies internal and external threats. The proposed regulation includes some of today's most effective cybersecurity practices. CrowdStrike applauds the inclusion of the following technologies and principles in the proposed regulation and recommends they continue to be included in the final regulation.

- **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.

- **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.

[3] *Request for Comment on Proposed 2nd Amendment to* 23 NYCRR *Part* 500, CrowdStrike, Jan 9, 2023. https://www.crowdstrike.com/wp-content/uploads/2023/02/New-York-Cyber-Amendment-Comments.pdf.

As the Department revises the proposed regulation, CrowdStrike recommends the consideration of the following principles and technologies as additional requirements for cybersecurity programs. Notably, several of these practices are also mandated in the May 2021 federal Executive Order (EO) 14028 on Improving the Nation's Cybersecurity.[4] We view the following as best practices for a comprehensive, risk-based, cybersecurity strategy.

- **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 to start, however; we recommend any language allow XDR as an option for organizations with advanced cybersecurity practices.

- **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.

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

- **Logging Practices**. Organizations should collect and retain security-relevant log information to support proactive security measures, threat hunting, and investigative use-cases.

- **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. The proposed regulation has MFA requirements to further protect entities from identity and credential theft attacks. As the proposed regulation recognizes, due to fundamental problems with today's widely-used authentication architectures, organizations must incorporate new security protections focused on authentication. Importantly, Zero Trust architecture and identity threat protection concepts are important adjuncts to MFA-based guidance because they radically reduce or prevent lateral movement and privilege escalation during a compromise, and can stop attacks even if legitimate credentials are compromised and MFA is bypassed.

Relatedly, the proposed regulation requires in-house developed applications use secure development practices. CrowdStrike views Security-by-Design and -Default principles as a positive change in driving greater security accountability for product makers. These principles are also a priority of the U.S. government. In April 2023, and updated in October 2023, the Cybersecurity and Infrastructure Security Agency ("CISA") and 17 international partners released a joint Secure-by-Design document which urges software manufacturers to take steps to design, develop, and deliver products that are secure from the very beginning of the process.[5] This concept was then adopted in the National Cybersecurity Strategy, both as a priority and as a means to accomplish other goals of the Strategy to secure the ecosystem.[6] We recommend that engineers building

[5] *Secure-By-Design*, CISA, October 2023. https://www.cisa.gov/resources-tools/resources/secure-by-design
[6] *National Cybersecurity Strategy*, White House, March 2023. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

applications reference the material publicly available from CISA, and other government agencies, on Security-by-Design and -Default principles to inform best practices in building secure applications.

B. Incident Reporting Timeline

The proposed regulation states:

> "The hospital CISO or their designee shall notify the department within two hours of a determination that a cybersecurity incident, as defined herein, has occurred and has had a material adverse impact on the hospital, in a manner prescribed by the department. All notifications to the department under this section does not replace any other notifications required under State or Federal law."

Due to the complex nature of cybersecurity incidents, organizations often do not know the full extent of impacts at the immediate point of detection. In recognition of this, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA"), and the DFS's newly implemented cybersecurity regulations, both require reporting an incident within 72-hours.

Given that this timeframe is emerging as a best practice, both in the U.S. and internationally, we recommend that the Department align its requirement to a 72-hour notification timeline in future drafts of the proposed regulation. While we believe strongly that time is of the essence in detecting and remediating cybersecurity incidents, we encourage policymakers and regulators to allow victim organizations to focus on response rather than reporting in the immediate wake of an incident. Allowing reasonable time for victims to understand and mitigate threats also ultimately supports higher-fidelity reporting and reduced impacts overall.

C. Reporting and Definition Harmonization

The Department has not drawn from an existing "cybersecurity incident" definition, or noted alignment with forthcoming federal definitions, but rather has created a new definition. As the Department reviews this proposed regulation, and drafts other pieces of regulation, CrowdStrike urges alignment where possible with existing rules and regulations. The proposed regulation has the opportunity to strengthen cybersecurity for organizations that play critical roles in the everyday lives of many New Yorkers.

Nonetheless, the new regulation will not be issued in a vacuum, but a variety of cybersecurity regulations. We recommend the Department align future drafts with CIRCIA's cybersecurity incident definition, and its forthcoming implementing regulation.

CrowdStrike recommends clarifying that there is no obligation to report "cybersecurity events," as currently defined. As the draft notes, there are significant distinctions between cybersecurity events and incidents, and reporting of issues mitigated or resolved at the event-level is unlikely to provide additional value.

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. 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
Manager, Public Policy

Email: policy@crowdstrike.com

***