REQUEST FOR COMMENT RESPONSE

Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies

File Number S7-04-22

May 22, 2023

I. INTRODUCTION

In response to the Securities and Exchange Commission's ("SEC") request for feedback on the proposed Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies ("proposed rule") 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 SEC's efforts to improve the cybersecurity practices of market entities such as brokers and dealers, investment companies, and investment advisers. Last year, CrowdStrike submitted comments on the SEC's proposed rule on "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure."[1]

The SEC appropriately notes in the proposed rule introduction that 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. Further, we found a 112% 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

[1] https://www.crowdstrike.com/wp-content/uploads/2023/02/2022_05_09_SEC-Cybersecurity-Risk-Mgmt.pdf.

vulnerabilities.[2] As adversaries continue to evolve and find new ways to target victims, organizations must increase their emphasis on cybersecurity practices that leverage the most effective technologies.

While adversary threats are growing, the legal and regulatory environment surrounding cybersecurity is growing increasingly complex. This follows from: (i) growing reliance on globally-distributed infrastructure, and (ii) increasing compliance obligations nationally and internationally. In order to ensure robust and effective cybersecurity outcomes, regulators must ensure compliance obligations remain feasible and 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 SEC as it considers the proposed rule.

A. Definition of Cybersecurity Incident

In the proposed rule, the SEC offers definitions for terms including "cybersecurity incident." We recommend that instead of creating new definitions, the SEC uses the definitions forthcoming in the Cybersecurity and Infrastructure Security Agency's (CISA) implementation of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) to streamline the reporting process. We recommend the SEC, and CISA, endeavor to achieve balance in scoping reportable incidents. The volume of resulting incident reports should be sufficient to discover and alert entities about systemic and/or widespread incidents; but the volume should not be so great as to create "noise" for analysts and extra work those impacted by low-impact commodity threat activity.

In cybersecurity, an important distinction exists between alerts and incidents, which should help inform notification scenarios and regulations. In most cases, organizations using contemporary cybersecurity solutions are alerted to malicious activity occurring in their environment. The nature of these alerts may vary, and could cover something like the installation of malicious software on one system, or the compromise of a single account. In scenarios where defenders see these alerts and address them quickly, the alert may not rise to the threshold of a cybersecurity "incident," where the threat actor has not meaningfully achieved their objective, accessed sensitive information, and the like. As such, CrowdStrike recommends that a covered incident only be defined as a substantial cyber incident and the SEC not create two tiers of definitions.

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

The SEC notes in the proposed rule that the "broad" proposed definition is purposeful. From our vantage point, for reasons described above, this is likely to lead to a "noise" from reporting volume.

Finally, there will be harmonization recommendations resulting from the ongoing work of the Cyber Incident Reporting Council, which was created by CIRCIA, to align federal cyber incident reporting structures. The SEC should follow these forthcoming recommendations in the drafting and implementation of the proposed rule.

B. Reporting Requirements

The proposed rule, as written, would require covered entities to give the SEC immediate written notice of a cybersecurity incident - this timeline does not allow for organizations to understand any component of the incident or even validate that an incident has occurred. Due to the nature of cybersecurity incidents, organizations often do not know the full extent of impacts at the immediate point of detection. For example, an incident where a threat actor gains access to a single resource but is not able to move laterally due to strong security practices likely would have a minor impact on the covered entity. Whereas, another incident in which a threat actor gains access, successfully moves laterally, establishes persistence, and is able to compromise a broader set of systems may have a severe impact. While these are important distinctions, the two incidents could look similar in the early investigation stage.

Consideration of the impact and severity of an incident is important not only when initially assessing evidence of an intrusion but also in discerning the efficacy of mitigation measures. Consequently, it is extremely difficult, if not impossible, for an organization to make a report with any meaningful information "immediately."

CIRCIA requires 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 SEC introduce a 72-hour notification timeline in future drafts of the proposed rule. While within 72-hours an organization likely will not be able to understand the full scope of an incident, it allows for enough investigative time for information of value to be shared. The SEC has also proposed that a report of the incident be due within 48-hours of initial notification. We respect the idea of a follow up report as new information about the incident is discovered; however, we suggest the SEC align with CIRCIA's timeline for a supplemental report.

Finally, CrowdStrike would like to emphasize that the "duty to report" is the responsibility only of the impacted covered entity, which includes third-parties hired by the impacted

covered entity to assist in the case of an incident. An organization should not report on behalf of another organization unless engaged by the impacted entity for that purpose. Due to the complexity of cyber incidents and modern IT enterprise environments, a third-party would not have enough relevant information to submit reports.

C. Publicly Disclosed Information

The proposed rule requires covered entities to publicly disclose a summary of their cybersecurity risks and an explanation of how those risks could affect business operations. The proposed rule goes on to require a more detailed analysis of these risks. While it could be a helpful exercise for an organization to review their cybersecurity risks internally to update plans and procedures, publicly disclosing cybersecurity weaknesses could enable threat actors to conduct malicious activities. Given that many cyber risks involve third parties (e.g., end-of-life software applications, breaches of providers, etc.) users sometimes face constraints in addressing them. Public disclosure in these instances may have an adverse effect on security.

Finally, we would like to emphasize that publicly disclosing an ongoing cyber incident could negatively impact remediations and investigations. In many instances, investigators prefer deliberate, tightly-sequenced actions – including public notifications – to maximize chances of a successful remediation or follow-on enforcement actions.

D. Cybersecurity best practices

The SEC's proposed rule creates requirements for covered entities to create cybersecurity policies that properly address their cybersecurity risks. We view the following technologies as key steps to defend against cyber threats. Notably, several of these practices are also mandated in the May 2021 federal Executive Order (EO) 14028 on Improving the Nation's Cybersecurity.[3]

- **Cloud Services**. Leveraging cloud systems provides a series of potential security enhancements. Retiring legacy applications and infrastructure reduces attack surface and points of failure. Cloud systems enable comprehensive visibility of workloads. For security technologies specifically, native cloud-based solutions provide robust and scalable protection of distributed environments.

[3] 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/.

- **Extended Detection & Response (XDR).** Cybersecurity threats are exceptionally broad, and for too long industry players have focused on narrow solutions. No single-purpose network appliance, software agent, or other security tool 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 other security-relevant data, wherever it exists within the enterprise. EDR is a natural baseline security capability, but XDR drives more comprehensive cybersecurity outcomes.

- **Machine Learning-Based Prevention**. The core of next-generation cybersecurity solutions is the ability to defeat novel threats based on behavior cues rather than known signatures. Machine learning and artificial intelligence are essential to this end. Leveraging these technologies is essential to meeting constantly-evolving threats.

- **Identity Threat Protection**: 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 identify and prevent identity-based attacks.

Additionally, there are multiple security program requirements that bolster organizations' security posture:

- **Speed**. When responding to a security incident or event, every second counts. The more defenders can do to detect adversaries at the outset of an attack, the better the chances of preventing them from achieving their objectives. Adversaries work rapidly at the outset of breach to move laterally and escalate privileges, seeking to gain access to more systems and data and ensure persistence. This means that organizations should measure and reduce their response time.[4]

[4] Elite organizations seek to identify a breach attempt within one minute, investigate within ten minutes, and isolate or remediate threats within sixty minutes.

- **Threat Hunting**. Whether through supply chain attacks or otherwise, adversaries periodically breach even very-well defended enterprises. However, properly trained and resourced defenders can find them and thwart their goals. Proactive hunting is a leading indicator of the strength of an enterprise cybersecurity program. Central to hunting is properly instrumenting enterprises to support both automated and hypothesis-driven adversary detection. The better-instrumented the environment, the more chances defenders give themselves to identify malicious activity as an attack progresses through phases. Multiple opportunities for detection increase defenders' chances of success and help avert "silent failures."

- **Zero Trust Architecture.** Due to fundamental problems with today's widely-used authentication architectures, organizations must incorporate new security protections focused on authentication. Zero Trust architecture concepts radically reduce or prevent lateral movement and privilege escalation during a compromise.

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

- **Managed Service Providers**. Some entities lack the cybersecurity maturity to run robust security programs internally, or seek to apply internal IT/security resources toward domain-specific challenges. Increasingly, such entities should rely upon managed security service providers to strengthen their security posture.

III. CONCLUSION

The SEC's proposed rule represents a strong preliminary attempt to strengthen security outcomes in a complex legal and policy environment. As the SEC moves forward, we recommend continued engagement with stakeholders. Finally, because the underlying technologies evolve faster than law and policy, we recommend that to the extent possible, requirements 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

***