CROWDSTRIKE

REQUEST FOR COMMENT RESPONSE

Securities and Exchange Commission (SEC): Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

May 9, 2022

I. INTRODUCTION

In response to the SEC's request for comments on its proposed amendments to risk management, incident reporting, and related disclosure issues, CrowdStrike, Inc. (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 threat 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 commend the SEC for seeking to improve cybersecurity and cybersecurity transparency for public companies and shareholders. CrowdStrike's observations support SEC findings regarding the increases in cybersecurity incidents in recent years.[1] Data breaches and other significant incidents continue to evolve and have increased over time. Given business impacts, cybersecurity has clearly emerged as a key corporate risk area and a Board-level issue.[2]

---

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

[2] Drew Bagley, *Insight into Cybersecurity Regulations is Critical for Today's Board Members*, Law (Sept. 12, 2018), https://www.law.com/global-leaders-in-law/2018/09/12/insight-into-cybersecurity-regulations-is-critical-for-todays-board-members/.

The legal and regulatory environment surrounding cybersecurity is increasingly complex on account of (i) reliance on globally-distributed infrastructure, and (ii) compliance obligations for 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.

A. Material Cybersecurity Incident Reporting Requirements

We commend the SEC for seeking to provide transparency to investors about material cybersecurity incidents that may impact a public company. However, we caution that cybersecurity incidents often take time to assess and mitigate. Moreover, there exists today a threshold distinction in sector and data-specific notification standards between a duty to notify a regulator versus a duty to notify an individual where an incident such as a data breach has occurred. Here, although the materiality threshold seeks to make a meaningful distinction between incident types, the effect of the public nature and four business day timeline of filing a Form 8-K, as opposed to another reporting method, risks mandating the publication of incomplete information during a volatile time period in an incident investigation.

We appreciate the thought put into qualifying the proposed notice obligation to incidents that may be "material" to a company's investors. We also appreciate the list of examples the SEC provided outlining what may be considered a material cybersecurity incident. However, cybersecurity incidents are not homogenous; no two significant incidents have the same impacts or effects. The process of evaluating materiality may take time, and, in some cases reducing where possible the negative impact of an incident, often can require substantially more time than four business days following the discovery of an incident.

Threat actors may choose to target an organization in a series of steps, rather than in a single attack. An initial intrusion into an enterprise is often not a threat actor's end goal. Instead, threat actors may first deploy a backdoor, harvest credentials, or use other methods in order to move laterally throughout a network and to their ultimate objective, such as accessing key data or altering source code. A threat actor may be stopped at any of the steps in the kill chain, and this raises important questions about impacts.

We recommend the SEC consider increasing the timeframe proposed in the new rule at least under certain circumstances. In some instances, the same personnel who are involved in performing remediations would be the same personnel responsible for authoring or contributing to disclosure items. Optimally, organizations should prioritize remediation activities, particularly where critical functions or sensitive personal data remain at risk. Further, to the extent that the victim organization itself is a software provider or supplier, an incident may impact downstream customer/user security as well. Here, all parties, including investors within the victim organization, have equities in prioritizing attention to the security of customers/users.

Incident reporting obligations are expanding over time, and companies may already be reporting cybersecurity incidents to other regulators and incurring reporting costs. While sector specific reporting requirements, *e.g.*, within the Health Insurance Portability and Accountability Act of 1996 (HIPAA), have long conferred reporting obligations on regulated entities, the passage of incident reporting legislation[3] in March has recently and significantly reshaped reporting obligations for a broad cross-section of organizations within the critical infrastructure space.

Within the private sector, longer-term disclosure norms have emerged over time within adjacent areas. For example, in general, security researchers make a 90 day allowance following the discovery and reporting of a vulnerability in another vendor's software.[4] Even when vulnerabilities are being actively exploited, organizations would 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 bigger impact (such as in vulnerability disclosure).

---

[3] Consolidated Appropriations Act 2022, H.R. 2471, 117th Cong. DIV Y, Cyber Incident Reporting for Critical Infrastructure Act of 2022 (2022), https://www.congress.gov/bill/117th-congress/house-bill/2471/text.

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

Accordingly, if the SEC were to add a reporting requirement on a Form 8-K with respect to incidents, the disclosure period should only begin after the reporting company is reasonably certain that necessary remediation actions have been completed and there is no longer an ongoing risk of harm from an ongoing incident. Additionally, it is important for any new rule to acknowledge that there may be circumstances in which an incident may not be material but where companies already face a duty to report a cybersecurity incident to a regulator. Consequently, a duty to report to a regulator by one standard may not necessarily mean an incident is material.

Finally, any discussion of materiality should explicitly acknowledge two key distinctions:

- **Alerts versus incidents**. In most cases, those using contemporary cybersecurity solutions should be 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 endpoint or system, or the compromise of a single account. In scenarios where defenders see these alerts and address them quickly, then frequently such an issue does not meet any reasonable standard of a cybersecurity "incident," where the threat actor has not meaningfully achieved their objective, accessed sensitive information, and the like.

- **Impacts versus serious impacts**. Not all breaches have the same level of severity. For example, an incident where a threat actor sees a list of user names might have a small or negligible impact on affected parties. Whereas, another incident in which a threat actor exfiltrates complete financial or medical records may have a severe impact. Consideration of the impact and severity of a breach is important not only when initially assessing evidence of an intrusion but also in discerning the efficacy of mitigation measures. Consequently, this criteria should explicitly inform risk determinations in assessing whether or not an incident is material not only at the time of discovery but also in ensuing timeframes as the scope of impact evolves.

B. Cybersecurity Risk Management Practices

We commend the SEC for strengthening cybersecurity by amplifying attention given to this issue, increasing transparency, and clarifying expectations. There are some key steps organizations should take to strengthen their security posture. These include:

- **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.

- **Identity Protection and Authentication**: As organizations embark on a digital transformation to work from anywhere models, Bring-Your-Own-Device policies become commonplace, and cloud services

multiply, 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.

- **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.

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

- **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.

Notably, many of today's most effective cybersecurity practices are outlined in the May 2021 Executive Order (EO) 14028 on Improving the Nation's Cybersecurity.[5]

Finally, we agree with the SEC's proposal to amend Item 407 of Regulation S-K to require disclosure about the extent to which registrants' board of directors include

[5] 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/.

members with cybersecurity expertise. Based on our experience working with numerous listed companies, Board-level cyber expertise addresses three common security program failure modes:

1. **Atrophy through inattention**. Cybersecurity is a process that requires ongoing attention. Concerted interest and oversight from the highest levels of organizations' leadership ensure that security programs remain robust and continue to meet constantly-evolving threats and risks.

2. **Compliance but ineffective security**. Companies could design programs that technically meet existing or proposed compliance requirements, but do not in practice effectively address threats or mitigate risks. The focus of boards of directors on outcomes can proactively address weak or eroding performance.

3. **Misaligned business conditions**. 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.

III. CONCLUSION

The SEC's proposed amendments represent a thoughtful attempt to strengthen security outcomes in a complex legal and policy environment. Cybersecurity risk management and incident remediation are difficult topics, and any new requirements will have a significant impact on affected companies. With an emphasis on adoption of practical security practices and a balanced approach to new reporting obligations, these adjustments can raise the bar of cybersecurity for companies and investors' expectations alike. As the SEC moves forward, we recommend continued engagement with stakeholders.

IV. ABOUT CROWDSTRIKE

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/.

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

Robert Sheldon
Director, Public Policy & Strategy

Email: policy@crowdstrike.com

***