Six Key Takeaways from the SEC's Most Recent Proposed Cybersecurity Rules for Registrants

March 14, 2022

On March 9, 2022, the SEC released its newest series of proposed cybersecurity rules, this time for all public companies. Consistent with the proposed rules issued last month for investment advisers and funds, which we discussed here, the SEC continues to prioritize cybersecurity disclosures to the marketplace, placing particular emphasis on timely and detailed disclosures of material cybersecurity incidents, as well as on periodic disclosures about cybersecurity risk management and governance.

These detailed and broadly applicable proposed rules (which have registered dissent from Commissioner Hester Pierce) significantly expand upon the SEC's 2018 statement and interpretive guidance for public companies on cybersecurity disclosures by promulgating a substantial new cybersecurity regulatory framework that creates significant new disclosure obligations for these entities. The proposed rules represent another step in the SEC's overarching strategy to create cybersecurity regulations for entities within the SEC's jurisdiction.

Key Requirements Under the Proposed Rules

- Current Disclosure of Material Cybersecurity Incidents on Form 8-K. Most notably, the proposed rules would require a registrant to disclose certain information about a material cybersecurity incident in a new Form 8-K line item within four business days of determining that a cyber incident it has experienced is material, rather than upon the discovery of the incident. Proposed Item 106(a) of Regulation S-K defines "cybersecurity incident" to include any "unauthorized occurrence on or conduct through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability" of the registrant's information or information systems. The SEC noted that this definition should be broadly construed to include accidental data exposures, deliberate action to gain access to systems or steal/alter data, or other system compromises or data breaches.

  To address any concern that some registrants may delay assessing materiality to avoid a disclosure obligation, proposed Item 1.05 requires the determination of

materiality to be made "as soon as reasonably practicable after discovery of the incident." The proposed rules would require these disclosures to include to the extent the information is known at the time of the 8-K filing: (1) the date the incident was discovered; (2) whether the incident is ongoing; (3) a brief description of the nature and scope of the incident; (4) an indication of whether any data was compromised; and (5) the potential effect of the incident on operations.

The proposed rules incorporate the well-settled Supreme Court precedent on materiality. Recognizing the fact-specific nature of the materiality inquiry, the proposed rules provide several examples of cybersecurity incidents that could be subject to disclosure, including business email compromises, data theft by internal or external actors, or ransomware. Notably, while the proposed rules would not provide a safe harbor for a reporting delay in the context of an ongoing internal or external investigation (such as one by law enforcement), they would provide for certain limited safe harbors, including from liability under Exchange Act Section 10(b) and Rule 10b-5 thereunder and protection against loss of Form S-3 or Form SF-3 eligibility. Additionally, while foreign private issuers are not required to file current reports on Form 8-K, General Instruction B of Form 6-K would be amended to reference material cybersecurity incidents among the items that may trigger a current report on Form 6-K.

- Periodic Updates to Disclosures of Cybersecurity Incidents. Proposed Item 106(d)(1) to Regulation S-K would also require a registrant to disclose any material changes in the registrant's Quarterly Report on Form 10-Q or Annual Report on Form 10-K from the disclosures made in the initially filed Item 1.05 8-K. This may include changes in scope, additional information on whether data was altered or stolen, and the steps taken to address the incident. Further, the proposed rules provide a non-exhaustive list of potential disclosures that should be addressed in a registrant's 10-Q or 10-K filings following a cybersecurity incident, including any material or future impact on operations and financial condition, status of the remediation efforts, and any changes to the registrant's cybersecurity policies and procedures because of the incident.

  Proposed Item 106(d)(2) of Regulation S-K would also require periodic disclosure of immaterial cybersecurity incidents that become material in the aggregate. Such matters could potentially include coordinated smaller but continuous cyber-attacks such as extended phishing campaigns or account takeovers if the registrant determines that the incidents are material in the aggregate. Similar to an Item 1.05 8-K disclosure for a single material event, these periodic disclosures should briefly describe the nature and scope of the incidents, whether data was stolen or altered, the impact to operations, and remediation efforts.

- Periodic Disclosure of Risk Management and Governance. Proposed Item 106(b) and (c) of Regulation S-K would also increase the scope and detail of registrant disclosures on cybersecurity risk management, strategy, and governance.

  - *Risk Management*. If adopted as is, proposed Item 106(b) of Regulation S-K would require "consistent and informative disclosure regarding [registrant] cybersecurity risk management and strategy[,]" potentially including disclosure of policies and procedures to manage cybersecurity risk. More specifically, to the extent applicable, registrants would be required to disclose the existence of a risk assessment program, engagement of any third-party auditors or consultants associated with the program, policies and procedures associated with third-party risk, and among other items, steps taken to prevent, detect, and minimize the effects of cybersecurity incidents.

  - *Governance*. Under proposed Item 106(c) of Regulation S-K, registrants would also be required to disclose their cybersecurity governance policies, including a discussion of the board and management's role in identifying, assessing, and managing cybersecurity risk, as well as their experience in dealing with such risks. More specifically, as it pertains to the board's oversight, registrants would be required to identify: (1) which board committee or directors are responsible for overseeing cybersecurity risks; (2) how the board is informed of cybersecurity risks; and (3) whether and how the board, or relevant body, "considers cybersecurity risks as part of its business strategy, risk management, and financial oversight." Additionally, the proposed rules would amend Item 407 of Regulation S-K such that registrants would also be required to disclose whether any of its directors have prior work experience, education, or knowledge, skills or other background in cybersecurity.

    Similarly, from a management perspective, the proposed rules would require that registrants disclose whether the registrant has a dedicated CISO, which positions or committees are responsible for detecting, managing, and responding to cybersecurity risk and their corresponding policies and procedures, including the frequency that such committees present to the board on cybersecurity risks.

Key Takeaways

- **Incident Response Planning**. While the proposed rules clarify that the four-day clock starts from the time that materiality is determined rather than from the time the incident is identified, the facts required to assess the impact of incidents must be timely escalated to the appropriate parties internally to make the materiality

determination. Registrants should review their incident response plans to ensure that they contain an escalation path to the legal and executive teams responsible for assessing materiality.

- **Assess Materiality Thresholds**. The SEC's commentary makes clear that it understands that materiality is case- and company-specific. Nonetheless, companies should consider leveraging their cybersecurity risk management programs and business continuity programs to evaluate the different cybersecurity risks facing the company and assess the operational, financial, and reputational impact of each type of incident. Understanding the costs of what could go wrong before the incident can help companies establish thresholds for materiality in advance, allowing the company to focus its resources on restoration and mitigation when the incident occurs.

- **Prepare Templates**. While the disclosure in each Item 1.05 8-K will be specific, certain aspects of the disclosure are likely to be the same from incident to incident. Similar to pre-prepared holding statements for customer, investor, or employee communications during an incident, companies should consider what language they can prepare in advance of any incident.

- **Disclosures and Evidence Preservation**. The proposed rules emphasize the importance of clear, accurate, and consistent disclosure regarding cybersecurity risk and incidents to investors and the SEC, formalizing takeaways from the SEC's 2021 enforcement actions in Pearson and First American. As it has in the past, the SEC will likely use the proposed rules once enacted to scrutinize cybersecurity disclosures and bring enforcement actions concerning deficiencies in cyber disclosures. Companies should ensure that their disclosures are not only accurate, but also are supported by objective evidence and documentation, which will require some thoughtful analysis as to over which aspects of the investigation the company wishes to assert privilege.

- **Test and Train at All Levels**. The proposed rules build on the SEC's 2018 guidance regarding the board's involvement in overseeing cybersecurity risk and emphasize the need for both the board and management to understand cybersecurity risk and the steps being taken to mitigate it. As companies continue to test their incident response plans and procedures, companies should consider including both management and the board in tabletop exercises, allowing these key players an opportunity to better understand their roles and responsibilities before, during, and after a cybersecurity incident.

- **De Facto Cybersecurity Standards**. Unlike the SEC's proposed rules for registered investment advisers, the SEC has not proposed any substantive cybersecurity

requirements for public companies. Despite this, the proposed disclosure requirements are still likely to impact the cybersecurity practices of public companies as the increase in disclosures by registrants will likely reveal common cybersecurity risk mitigation frameworks, practices, and tools. Companies should consider evaluating their cybersecurity programs against known industry standards in anticipation of such public disclosures and take appropriate steps to align their practices.

We will continue to track and blog on these important issues. Public comments are open until at least May 9, 2022.

* * *

To subscribe to our Data Blog, please click here.

The authors would like to thank Debevoise law clerk Kevin Hayne for his contribution to this post.

WASHINGTON, D.C.

Luke Dembosky
ldembosky@debevoise.com

NEW YORK

Avi Gesser
agesser@debevoise.com

Matthew E. Kaplan
mekaplan@debevoise.com

Charu A. Chandrasekhar
cchandra@debevoise.com

Michael R. Roberts
mrroberts@debevoise.com

Rebecca Zipursky
rzipursk@debevoise.com

San Francisco

HJ Brehmer
hjbrehme@debevoise.com