SEC Adopts New Cybersecurity Rules for Issuers – Part 2 Key Takeaways

August 7, 2023

On July 26, 2023, the SEC adopted long-anticipated final rules on cybersecurity risk management, strategy, governance and incident disclosure for issuers ("Final Rules"). We summarized the key obligations under the Final Rules, and changes from the Proposing Release,[1] in our July 27, 2023 update. In this companion update, we discuss key takeaways across three areas for issuers to consider:

(1) Disclosure of material cybersecurity incidents: The Final Rules create a four-business-day obligation to disclose material incidents. Issuers should consider developing a well-informed and deliberative process to support the materiality analysis well before an incident occurs; adherence to internal practices and disclosure controls and procedures will aid issuers in establishing good faith compliance with the disclosure obligation.

(2) Cybersecurity risk management and strategy: The Final Rules require issuers to disclose more granular details of their cyber risk management than is common among issuers at present. Issuers should review their cybersecurity processes, how these processes are integrated with the issuer's overall risk management program, and how these relate to the issuer's cybersecurity risk profile to consider how the required disclosure will appear in the face of greater public scrutiny.

(3) Cybersecurity governance: The disclosure of senior management's and the board's roles in managing and overseeing cybersecurity will up the ante on expectations for cybersecurity oversight, including attracting, developing and retaining cybersecurity talent. Ensuring that both senior management and the board are informed and that their involvement is well-documented will be more important than ever.

[1] 87 Fed. Reg. 16590 (Mar. 23, 2022).

Disclosure and Amendment of Material Cybersecurity Incidents

Domestic issuers are required to disclose certain information about a material cybersecurity incident under new Item 1.05 of Form 8-K ("Item 1.05") within four business days of determining that a cybersecurity incident it has experienced is material. Cybersecurity incident disclosures should include a description of "the material aspects of the nature, scope, and timing of the incident, and the material impact or reasonably likely material impact on the issuer, including its financial condition and results of operations." The determination of materiality is to be made "without unreasonable delay" (as opposed to "as soon as reasonably practical," as was proposed). Foreign private issuers ("FPIs") that are required to furnish a Form 6-K must disclose on Form 6-K material cybersecurity incidents that they disclose or otherwise publicize in a foreign jurisdiction, to any stock exchange or to their security holders, promptly after the material contained in the report is made public.

- **Review the incident response plan and procedures to ensure that the materiality analysis is appropriately sequenced alongside other incident response activities and that materiality determination protocols are well-informed, deliberative and documented**. The Final Rules changed the required timing of the materiality determination from "as soon as reasonably practicable" to "without unreasonable delay." In doing so, the Commission acknowledged that materiality determinations may take time and require "an informed and deliberative process." However, it warned that "though the determination need not be rushed prematurely, it also cannot be unreasonably delayed in an effort to avoid timely disclosure."[2]

  Taken together, an issuer should consider: (1) carefully reviewing its incident response plan and procedures to ensure that the materiality determination is appropriately sequenced alongside incident fact finding, in accordance with the nature and scope of any given incident (*e.g.*, earlier if involving key systems and information or if a large volume of important data are implicated); (2) ensuring that its incident response resources are allocated such that any need for early information sharing with third-party stakeholders would not result in unreasonable delay of the materiality analysis; and (3) ensuring that there are well-reasoned bases for any changes to the incident response plans—including as it relates to any contemplated revisions to (a) incident severity assessment time, (b) criteria for escalation to management or board committees in charge of public disclosures or (c) materiality

[2] Rule Release, 37. The Commission's cited examples in the Rule Release are instructive on this point: For instance, for incidents that (1) impact key systems and information ("crown jewels") and (2) involve unauthorized access to or exfiltration of large quantities of particularly important data, the materiality determination should not be delayed because the issuer does not have complete information, is not able to determine the full extent of the incident, or needs to continue to investigate. The Commission also specifically warned against an issuer revising its existing incident response policies and procedures to support a delayed materiality disclosure.

determination protocols and processes, which should be well-informed and deliberative.

- **Develop a disclosure analysis framework that incorporates both qualitative and quantitative factors, that accounts for the broadened definition for "cybersecurity incident," and does not disclose information that would impede incident response and remediation**. The Commission noted in the Rule Release accompanying the Final Rule ("Rule Release") that the focus of the Item 1.05 disclosure should be "primarily on the impacts of a material cybersecurity incident, rather than on […] details regarding the incident itself."[3] The Commission also underscored the importance of considering both *qualitative* and *quantitative factors*, and both immediate and longer-term effects, in making such an assessment.[4] The Commission emphasized that a "lack of quantifiable harm does not necessarily mean an incident is not material,"[5] and that a cybersecurity incident involving foreseeable future harms may be material, even if the incident has not yet caused actual harm.

  The Final Rules and Rule Release embrace an expansive definition of "cybersecurity incident," which includes "a series of related unauthorized occurrences,"[6] and "an accidental occurrence […] even if there is no confirmed malicious activity."

  To satisfy these new disclosure requirements, issuers should consider developing a framework to structure and guide materiality and disclosure analysis and decisions for each incident, accounting for potential serial unauthorized occurrences and accidental occurrences. Such a framework may be incorporated into the issuer's existing disclosure controls and procedures, and should facilitate a well-informed and deliberative analysis of the incident, such as by mapping to enumerated qualitative and quantitative factors for actual and likely harm.

  Issuers should also consider Instruction 4 to Item 1.05 when developing incident disclosures, which provides that issuers "need not disclose specific or technical information about its planned response to the incident or its cybersecurity systems,

---

[3] Rule Release, 29.

[4] Rule Release, 80. The Commission provided certain *illustrative* materiality assessment factors, including: (1) harm to an issuer's reputation, customer or vendor relationships, and competitiveness (Rule Release, 29); (2) possibility of litigation or regulatory investigations or actions (including by state, Federal authorities, and non-U.S. authorities) (Rule Release, 29-30); (3) data theft (and resulting scope or nature of harm to individuals, customers, or others) (Rule Release, 37), asset loss, IP loss (Rule Release, 29-30); and (4) financial impact (Rule Release, 32).

[5] Rule Release, 37.

[6] Rule Release, 76. (Noting that a series of related unauthorized occurrences could take place and be considered material in the aggregate where (1) "the same malicious actor engages in a number of smaller but continuous cyberattacks related in time and form and against the same company" or (2) multiple actors exploit the same vulnerability and collectively impede the company's business.)

related networks and devices, or potential system vulnerabilities in such detail as would impede the [issuer's] response or remediation of the incident."

- **Review policies and procedures regarding the triage and escalation of third-party cybersecurity incidents to enable prompt materiality analysis, where appropriate**. The Commission specifically declined in the Rule Release to exempt "registrants from providing disclosures regarding cybersecurity incidents on third-party systems they use" or to provide "a safe harbor for information disclosed about third-party systems."[7] As a result, issuers should be prepared to promptly conduct an independent materiality analysis upon becoming aware of a third-party cybersecurity incident, as "disclosure may be required by both the service provider and the customer (registrant), or by one but not the other, or by neither."[8] To address this requirement, issuers should consider integrating any third-party cybersecurity incident notification and internal escalation processes into their materiality determination protocol and disclosure controls and procedures. The Commission advised that an issuer should only disclose based on information available to it, and that an issuer is not required to conduct additional inquiries outside of its regular channels of communication with third-party service providers pursuant to its contracts and in accordance with the issuer's disclosure controls and procedures.

- **Track any missing required information in the initial Form 8-K filing and establish a cadence to review ongoing material incidents**. Instruction 2 to Item 1.05 of Form 8-K allows issuers to omit disclosure of otherwise required information from an initial Form 8-K filing where such information is not determined or available at the time. An issuer is required to include a statement to this effect in the initial filing and must provide such information in a Form 8-K amendment within four business days of determining such information, without unreasonable delay, or of such information becoming available. Issuers should therefore (1) closely track any gaps in required elements in the initial Form 8-K filing; (2) establish a cadence for reviewing ongoing material incidents for any of the initially missing information; and (3) when such information is identified, disclose them in an amended Form 8-K.

  Note that issuers remain subject to the separate obligation to correct any prior disclosure that is subsequently discovered to be untrue (or to have contained material omissions) *at the time the disclosure was made* (the so-called "duty to correct"). Issuers should also be mindful of the need to update a disclosure that becomes materially inaccurate after it is made (the so-called "duty to update").[9] The Rule Release acknowledges that issuers do not have a general continuous disclosure

[7] Rule Release, 31.

[8] Rule Release, 31.

[9] Rule Release, 52.

obligation, but suggested that issuers "should consider whether they need to revisit or refresh previous disclosure, including during the process of investigating a cybersecurity incident," particularly in the context of newly required Form 10-K and Form 20-F disclosure, as further described below.

Cybersecurity Risk Management & Strategy

Issuers, including FPIs, will be required to describe on Forms 10-K, 10-Q,[10] and 20-F, as applicable, their cybersecurity risk assessment and management processes and whether risks from cybersecurity threats have materially affected or are reasonably likely to materially affect the issuer. Issuers should review their cyber risk assessment processes and consider how they will appear alongside industry benchmarks and peer issuers' disclosures.

- **Consider steps to align cybersecurity risk management processes with industry standards**. According to the Rule Release, issuers are expected to disclose "whatever information is necessary, based on their facts and circumstances, for a reasonable investor to understand their cybersecurity processes."[11] To help position their processes and related disclosure favorably in an established context, issuers should consider benchmarking their cybersecurity risk management processes against industry standards such as the NIST and ISO frameworks. Be prepared to bridge any gaps accordingly.

- **Consider engaging outside vendors to augment cybersecurity capabilities, as appropriate**. Many issuers already outsource elements of their risk management, risk assessment, or monitoring and response to cyber events (*e.g.*, Security Operations Center, Managed Security Service Provider, or incident response vendors, among others). New Item 106(b)(ii) of Regulation S-K requires disclosure of "[w]hether the registrant engages assessors, consultants, auditors, or other third parties in connection with [the firm's cybersecurity] processes." Issuers should consider how their disclosures regarding the use of internal versus third-party resources will compare to those of industry peers. Issuers should also take steps to ensure that internal documentation of services provided is consistent with the description of those services in periodic disclosures.

[10] While the Final Rule does not contain affirmative Form 10-Q disclosure obligations, the Rule Release references the 2018 Interpretive Release, wherein "the Commission reiterated that registrants must provide timely and ongoing information in periodic reports (Form 10-Q, Form 10-K and Form 20-F) about material cybersecurity risks and incidents that trigger disclosure obligations." Rule Release, 113-14.

[11] Rule Release, 63.

- **Consider enhancing oversight of third-party service providers and management of cybersecurity risks presented by third-party servicers.** New Item 106(b)(iii) of Regulation S-K requires issuers to disclose "[w]hether the registrant has processes to oversee and identify [material cybersecurity] risks from cybersecurity threats associated with its use of any third-party service provider." Issuers that do not have existing third-party diligence and oversight processes should consider how their disclosures will compare to those of their peers on this topic. Firms with existing diligence and oversight processes should consider whether there are any gaps in execution or opportunities for enhancement.

Cybersecurity Governance: Management Responsibilities & Board Oversight

Issuers, including FPIs, will be required to describe the board's oversight of and management's role and expertise in assessing and managing material risks posed by cybersecurity threats in their Forms 10-K, 10-Q and 20-F, as applicable. Though the Final Rules' governance requirements are less prescriptive and granular than initially proposed, the Rule Release makes clear that the Commission expects issuers to consider several of the previously prescribed elements — including the frequency of board discussions of cybersecurity risks and designation of CISO — in their disclosures, to the extent material.

- **Consider documenting board discussions with management on cybersecurity.** The Final Rules require issuers to describe the processes by which the board is informed of cybersecurity risks. The Commission noted that discussion of the frequency of board discussions may be relevant to the description of the board processes, and issuers should thus consider inclusion of this information. Issuers should consider instituting a regular cadence (*e.g.*, quarterly) for such reporting where appropriate and should document management presentations to the board to support the disclosure of the board's oversight processes and the required disclosure under Item 106(c)(2)(iii) for management's reporting of information to the board.

- **Consider how best to describe management's cybersecurity expertise and training.** The Final Rules provide a non-exclusive list of items for issuers to consider when describing management's role in assessing and managing the issuer's material risks from cybersecurity threats. This list includes, as its first item, identifying the management positions or committees "responsible for assessing and managing such risks," and identifying "the relevant expertise of such persons or [committee] members in such detail as necessary to fully describe the nature of the expertise." Issuers should therefore consider how to accurately and effectively describe the experience of members of management who are responsible for cybersecurity. The

Final Rule provides a list of examples of expertise, including "[p]rior work experience in cybersecurity; any relevant degrees or certifications; [and] any knowledge, skills or other background in cybersecurity." To the extent necessary, firms also should consider how to support or supplement that expertise.

Compliance obligations for the majority of issuers begin after the later of 90 days from the date of publication (which is still forthcoming) or December 18, 2023. Smaller reporting issuers are given a longer period to come into compliance, with obligations effective after the later of 270 days from the effective date of the rules or June 15, 2024. For disclosures required in Forms 10-Q and 10-K and the comparable requirements in Form 20-F, issuers must begin providing disclosures with annual reports for fiscal years ending on or after December 15, 2023. Issuers must begin using Inline XBRL tagging one year after initial compliance with the related disclosure requirement.

The Final Rules are available here.

To subscribe to the Data Blog of our Data Strategy and Security practice, please click here.

* * *

Please do not hesitate to contact us with any questions.

NEW YORK

Charu A. Chandrasekhar
cchandrasekhar@debevoise.com

Avi Gesser
agesser@debevoise.com

Matthew E. Kaplan
mekaplan@debevoise.com

Erez Liebermann
eliebermann@debevoise.com

Benjamin R. Pedersen
brpedersen@debevoise.com

Paul M. Rodel
pmrodel@debevoise.com


Steven J. Slutzky
sjslutzky@debevoise.com


Matt Kelly
makelly@debevoise.com


Kelly Donoghue
kgdonoghue@debevoise.com


Chris Duff
ceduff@debevoise.com


John Jacob
jjacob@debevoise.com


Amy Pereira
apereira@debevoise.com

WASHINGTON, D.C.


Ned Terrace
jkterrac@debevoise.com


Luke Dembosky
ldembosky@debevoise.com

SAN FRANCISCO


Mengyi Xu
mxu@debevoise.com