Simpson Thacher

Regulatory and Enforcement Alert

SEC Proposes Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure Rules

March 11, 2022

On Wednesday, by 3-1 vote, the SEC approved proposed rules aimed at enhancing and standardizing disclosures made by public companies regarding cybersecurity risk management, strategy, governance and incident reporting,[1] reflecting the third rulemaking project the Commission has proposed in connection with cybersecurity in the past year.[2] The proposal, if adopted, would require mandatory reporting of material cybersecurity incidents and mandatory ongoing disclosures regarding companies' governance, risk management, and strategy with respect to cybersecurity risks.

By way of background, in October 2011, the Division of Corporation Finance issued guidance that addressed disclosure obligations relating to cybersecurity risks and incidents explaining that, although no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents, public companies nonetheless may be obligated to disclose material risks and incidents in various sections of their periodic reports, *e.g.*, their description of business, risk factors and management's discussion and analysis of financial condition and results of operation sections.[3] In 2018, the Commission issued interpretive guidance to reinforce and expand upon the 2011 Staff Guidance by identifying existing provisions in Regulations S-K and S-X that may require disclosure about cybersecurity risks, governance, and incidents.[4] Notably, the guidance did not create any new obligations.

While the guidance set forth in both the 2011 Staff Guidance and the 2018 Interpretive Release would remain in place if the Commission adopts the proposed rules, the rules would mark the first securities disclosure obligations on issuers that are specifically tailored to cybersecurity events. Most significantly, the rules contemplate the disclosure of certain cybersecurity events far sooner than currently required.

---

[1] *See* Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure as well as Public Company Cybersecurity Fact Sheet.

[2] On January 26, 2022, the Commission voted to propose expanding Regulation Systems Compliance and Integrity (SCI) to certain government securities trading platforms. Regulation SCI for ATSs That Trade U.S. Treasury Securities and Agency Securities. On February 9, 2022, the Commission voted to propose new obligations for registered investment advisers and funds with respect to cybersecurity. Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies.

[3] CF Disclosure Guidance: Topic No. 2 – Cybersecurity (Oct. 13, 2011).

[4] Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Release No. 33-10459 (Feb. 26, 2018) No. 33-10459 (Feb. 21, 2018) [83 FR 8166].

The proposed rules:

- Expand Form 8-K to add a new Item 1.05, which would require registrants to disclose information about a material cybersecurity incident within four business days after the registrant determines that it has experienced a material cybersecurity incident. An Item 1.05 8-K would be triggered on the date a registrant determines that a cybersecurity incident is material, rather than the date of discovery of the incident;
- Expand Regulation S-K to include new Item 106(d), which would apply to both Forms 10-K and 10-Q, to provide updated disclosure relating to previously disclosed cybersecurity incidents and to require disclosure, to the extent known to management, when a series of previously undisclosed individually immaterial cybersecurity incidents has become material in the aggregate;
- Amend Item 407 of Regulation S-K to require disclosure in annual reports and/or proxy statements if any member of the registrant's board of directors has expertise in cybersecurity, naming such director and any detail necessary to fully describe the nature of the expertise.

The proposed rules also contemplate the application of enhanced cybersecurity reporting to foreign private issuers through changes to the Form 20-F and Form 6-K requirements.

For purposes of the proposed rules, the Commission has provided the following definitions of "cybersecurity incident," "cybersecurity threat" and "information systems" with respect to the proposed disclosure requirements.

- "*Cybersecurity incident*" is defined to mean an "unauthorized occurrence on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein."
- "*Cybersecurity threat*" is defined to mean "any potential occurrence that may result in, an unauthorized effort to adversely affect the confidentiality, integrity or availability of a registrant's information systems or any information residing therein."
- "*Information systems*" is defined to mean "information resources, owned or used by the registrant, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of the registrant's information to maintain or support the registrant's operations."

In advocating for the new rules, Chair Gensler described cybersecurity as "an emerging risk with which public issuers increasingly must contend," and further stated that "[t]he interconnectedness of our networks, the use of predictive data analytics, and the insatiable desire for data are only accelerating, putting our financial accounts, investments, and private information at risk. Investors want to know more about how issuers are managing those

growing risks."[5] In her dissenting statement, however, Commissioner Peirce cautioned that the proposal "flirts with casting [the SEC] as the nation's cybersecurity command center, a role Congress did not give [the SEC]."[6]

On the one hand, companies have been required—under longstanding disclosure requirements—to disclose material cybersecurity events in their periodic SEC filings, and the proposed rules do not impact those obligations. However, the proposed rules are noteworthy because, among other things, they create a specific Form 8-K trigger for cybersecurity incidents that will mandate prompt consideration and continued evaluation of the materiality of an incident. While the proposed rules tie the trigger for disclosure to the date upon which a materiality determination is made rather than the date of the discovery of the incident, we nonetheless anticipate in practice that the proposed rules may in certain circumstances mandate disclosure earlier in the lifecycle of an event when less information is known. The prospect of an extremely compressed time frame for assessing the materiality of an incident reinforces the importance of having a pre-packaged set of procedures in place that clearly define roles and responsibilities for responding to cyber incidents. This would likely require companies to consider and perhaps implement changes to their existing disclosure controls and procedures, an area where the SEC has been recently focused.[7] Moreover, the SEC's emphasis on the disclosure of board-level cybersecurity expertise and oversight will likely prompt public companies to assess the skill sets of their current and potential new directors with a new lens.

Conclusion

The Commission has made it clear that the economic risk and cost related to cybersecurity incidents has greatly increased since the Division of Corporation Finance issued its 2011 Staff Guidance and the 2018 Interpretive Release. Now, in an effort to achieve uniformity, the Commission has taken a bold step in proposing these more stringent cybersecurity rules. Given the Commission's new proposal and its continued focus on cybersecurity related disclosures, as well as the continuing guidance in the Interpretive Guidance in 2018, public companies should consider a fresh review of their disclosure controls and their cybersecurity policies and procedures to assess whether any modifications are warranted.

[5] SEC Chair Gary Gensler, Statement on Proposal for Mandatory Cybersecurity Disclosures.

[6] Commissioner Hester M. Peirce, Dissenting Statement on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Proposal.

[7] *See* Simpson Thacher, As Cyber Incidents Continue to Rise, the SEC Charges Issuer for Inadequate Disclosure Controls in the Context of a Data Breach as well as SEC Settles Charges With Pearson plc Relating to Disclosures Concerning Cyber Breach.

CONTACT THE AUTHORS

For further information about this Alert, please contact the following authors: Marc P. Berger, Brooke E. Cucinella, Nicholas S. Goldin, Karen Hsu Kelley, Lori E. Lesser, Joshua A. Levine, Charles Mathes, Michael J. Osnato, Jr., Shanice D. Hinckson, or any other member of the **Government and Internal Investigations Group, Privacy and Cybersecurity Practice** or **Public Company Advisory Practice** below.

CONTACTS

Antonio Bavasso
+44-(0)20-7275-6122
antonio.bavasso@stblaw.com

Martin S. Bell
+1-212-455-2542
martin.bell@stblaw.com

Marc P. Berger
+1-212-455-2197
marc.berger@stblaw.com

Stephen P. Blake
+1-650-251-5153
sblake@stblaw.com

Brooke E. Cucinella
+1-212-455-3070
brooke.cucinella@stblaw.com

Stephen M. Cutler
+1-212-455-2773
stephen.cutler@stblaw.com

Adam Goldberg
+852-2514-7552
adam.goldberg@stblaw.com

Nicholas S. Goldin
+1-212-455-3685
ngoldin@stblaw.com

Karen Hsu Kelley
+1-212-455-2408
kkelley@stblaw.com

Meaghan A. Kelly
+1-202-636-5542
mkelly@stblaw.com

Jeffrey H. Knox
+1-202-636-5532
jeffrey.knox@stblaw.com

James G. Kreissman
+1-650-251-5080
jkreissman@stblaw.com

Noritaka Kumamoto
+81-3-5562-6219
nkumamoto@stblaw.com

Lori E. Lesser
+1-212-455-3393
llesser@stblaw.com

Joshua A. Levine
+1-212-455-7694
jlevine@stblaw.com

Charles Mathes
+1-212-455-2258
charles.mathes@stblaw.com

Michael J. Osnato, Jr.
+1-212-455-3252
michael.osnato@stblaw.com

Karen Porter
+1-202-636-5539
karen.porter@stblaw.com

Cheryl J. Scarboro
+1-202-636-5529
cscarboro@stblaw.com

John Terzaken
+1-202-636-5858
john.terzaken@stblaw.com

Jonathan K. Youngwood
+1-212-455-3539
jyoungwood@stblaw.com

Shanice D. Hinckson
+1-212-455-2113
shanice.hinckson@stblaw.com