SULLIVAN & CROMWELL LLP

S&C memo

March 11, 2022

SEC Proposes New Cybersecurity Disclosure Rules for Public Companies

Proposed Rules Would Require Disclosure of Material Cybersecurity Incidents, as well as Cybersecurity Risk Management, Strategy and Governance Disclosures

SUMMARY

On March 9, 2022, the Securities and Exchange Commission proposed new rules (the "Proposed Rules") for registrants regarding disclosure of material cybersecurity incidents, as well as cybersecurity risk management, strategy and governance.[1] The Proposed Rules would require (1) disclosure in Form 8-K of information about a cybersecurity incident within four business days of determining that the incident is material, (2) updated disclosure in Forms 10-K and 10-Q of previously disclosed cybersecurity incidents, and disclosure of previously undisclosed, individually immaterial incidents when a determination is made that they have become material on an aggregated basis, (3) disclosure in Form 10-K of cybersecurity policies and procedures and governance practices, including at the board and management levels, and (4) disclosure of the board of directors' cybersecurity expertise. The Proposed Rules would subject foreign private issuers to the same disclosure requirements in their Form 20-Fs, and would amend Form 6-K to add "cybersecurity incidents" as a reporting topic.

If adopted, the Proposed Rules would represent a significant expansion of the SEC's current cybersecurity disclosure framework for registrants by adding more detailed and prescriptive requirements, which could have implications for corporate governance. The public comment period will be open until the later of May 9, 2022 or 30 days following the publication of the Proposing Release in the Federal Register.

BACKGROUND

Existing Disclosure Framework

In 2011, the SEC issued interpretive guidance noting that U.S. securities laws require disclosure of material computer-system intrusions and information-technology risks, even though the laws do not explicitly address cybersecurity. In response, many registrants began including cybersecurity-related disclosures in their annual and quarterly reports, often in the form of risk factors and forward-looking statement disclaimers. In 2018, applying its traditional principles-based approach, the SEC issued further interpretive guidance stating, among other things, that to the extent material, companies should specifically describe cybersecurity incidents and the nature of their boards' roles in overseeing management of cybersecurity risks and emphasizing the need for comprehensive disclosure policies and procedures relating to cybersecurity. Following the 2018 guidance, many registrants expanded their risk factors to focus on cybersecurity incidents and added disclosures regarding board or committee cybersecurity oversight to their proxy statements.[2] Although recognizing that disclosure has improved since 2018, the SEC staff maintains that reporting practices are inconsistent, may not be timely, and disclosure can be difficult to locate.

Purpose of the Proposed Rules

The SEC has become increasingly concerned in recent years about timely disclosure of cybersecurity risks and incidents as these risks and incidents have escalated significantly and continue to increase. In recent months, the SEC has issued several enforcement actions against companies alleging inadequate disclosure controls and procedures relating to cybersecurity.[3] In addition, following the discovery of the compromise of SolarWinds software, through which Russia infiltrated U.S. federal agencies and reportedly over 18,000 companies, the SEC asked registrants to respond to a series of questions concerning their response to the compromise and experience with certain other cybersecurity incidents.[4] SEC Chair Gensler has made clear in recent months that the SEC staff would propose new disclosure rules intended to enhance and standardize disclosure and to, in his view, "improve the overall cybersecurity posture and resiliency of the financial sector."[5]

The SEC noted in the Proposing Release that "cybersecurity is among the most critical governance-related issues for investors, especially U.S. investors."[6] In the SEC's view, "investors would benefit from more timely and consistent disclosure about material cybersecurity incidents," and "from greater availability and comparability of disclosure by public companies across industries regarding their cybersecurity risk management, strategy and governance practices in order to better assess whether and how companies are managing cybersecurity risks."[7] The Proposed Rules are intended to reflect these policy goals.

Broader National Context

The Proposed Rules coincide with new cybersecurity standards and disclosure requirements that have been issued across the federal government in the past nine months. These include:

- President Biden's *Executive Order on Improving the Nation's Cybersecurity*, which mandates cybersecurity standards and information-sharing on cybersecurity incidents for government service providers, among other requirements; [8]
- new cybersecurity standards and disclosure requirements imposed by the Department of Homeland Security for companies in a range of critical infrastructure sectors;[9]
- new rules adopted by federal and state banking regulators mandating disclosure to the agencies of certain significant cybersecurity incidents;[10]
- new guidance from the Treasury's Office of Foreign Assets Control that offers a mitigated enforcement response where a company that unknowingly made a ransomware payment in violation of sanctions regulations had an adequate cybersecurity program prior to the attack and disclosed and cooperated fully with law enforcement during and after the attack;[11]
- new guidance from the Treasury's Financial Crimes Enforcement Network ("FinCEN") stating that ransomware attacks and related transactions should be reported immediately to law enforcement and FinCEN;[12] and
- this month, following Russia's invasion of Ukraine, the Senate's passage of the *Strengthening American Cybersecurity Act,* which would mandate that critical infrastructure entities report certain cybersecurity incidents to the government within 72 hours.[13]

The Proposed Rules and other new federal requirements follow a series of high profile cybersecurity attacks that have harmed U.S. national security and the private sector in the past eighteen months. These include the SolarWinds attack; China's compromise of Microsoft Exchange, used throughout the U.S. public and private sectors; and the ransomware attack against Colonial Pipeline Co. by Russia-based actors that disrupted nearly half of the East Coast's delivery of diesel, gasoline and jet fuel in 2020. Russia's invasion of Ukraine is expected to increase the risk of additional cybersecurity attacks against the U.S. public and private sectors.

OVERVIEW OF THE PROPOSED RULES

New Form 8-K Requirements

The Proposed Rules would add a new Item 1.05 to Form 8-K that would require disclosure of material cybersecurity incidents within four business days after a registrant determines that it has experienced a material cybersecurity incident.

Content. Item 1.05 would require disclosure of the following information about the cybersecurity incident, to the extent known at the time of the filing:

- When the incident was discovered and whether it is ongoing;
- A brief description of the nature and scope of the incident;
- Whether any data was stolen, altered, accessed or used for any other unauthorized purpose;

- The effect of the incident on the registrant's operations; and
- Whether the registrant has remediated or is currently remediating the incident.

The Proposed Rules make clear that a registrant would not be expected to disclose specific, technical information about its planned response to the incident or its cybersecurity systems, related networks and devices or potential system vulnerabilities in such detail as would impede the registrant's response or remediation of the incident.

Timing. The disclosure requirement would be tied to the date the registrant determines the cybersecurity incident is material, rather than the date of discovery of the incident. However, a registrant would be required to make a materiality determination regarding a cybersecurity incident as soon as reasonably practicable after discovery of the incident. The SEC also proposes to amend Form S-3 to provide that untimely filing of an Item 1.05 Form 8-K would not result in loss of Form S-3 eligibility.

Materiality Determination. The Proposing Release underscores that although the materiality standard is well established, the analysis "is not a mechanical exercise" and "doubts should be resolved in favor of disclosure to investors." Registrants would need to consider both quantitative and qualitative factors, taking into consideration the total mix of information and all relevant facts and circumstances.

Examples of Incidents Requiring Disclosure. The Proposing Release includes broad, non-exclusive examples of incidents that may require disclosure on Form 8-K if material:

- An unauthorized incident that has compromised the confidentiality, integrity or availability of an information asset (data, system or network); or violated the registrant's security policies or procedures. Incidents may stem from the accidental exposure of data or from a deliberate attack to steal or alter data;
- An unauthorized incident that caused degradation, interruption, loss of control, damage to or loss of operational technology systems;
- An incident in which an unauthorized party accessed, or a party exceeded authorized access, and altered, or has stolen sensitive business information, personally identifiable information, intellectual property, or information that has resulted, or may result, in a loss or liability for the registrant;
- An incident in which a malicious actor has offered to sell or has threatened to publicly disclose sensitive company data; or
- An incident in which a malicious actor has demanded payment to restore company data that was stolen or altered.

No Reporting Delay for Ongoing Investigations. Consistent with the SEC's 2018 interpretive guidance, although an ongoing investigation may affect the content of the disclosure, the Proposed Rules would not permit a reporting delay for ongoing investigations, even where law enforcement has requested a delay and state law permits it, and regardless of the fact that the disclosure may provide malicious actors with information regarding the scope and status of the breach.

New Form 10-K and Form 10-Q Disclosure Requirements (For Foreign Private Issuers, Form 20-F and Form 6-K)

Requirement to Update Previously Disclosed Cybersecurity Incidents on Form 8-K. In order "to balance the need for prompt and timely disclosure regarding material cybersecurity incidents with the fact that a registrant may not have complete information about a material cybersecurity incident at the time it determines the incident to be material," proposed new Item 106 of Regulation S-K would require updated disclosure in Quarterly Reports on Form 10-Q and Annual Reports on Form 10-K of material changes, additions or updates to previously disclosed cybersecurity incidents.[14] A foreign private issuer that previously reported an incident on Form 6-K would be required to provide such updates in its Annual Report on Form 20-F pursuant to new Item 16J. Non-exclusive examples of the type of disclosure that should be provided, if applicable, include:

- Any material impact of the incident on the registrant's operations and financial condition;
- Any potential material future impacts on the registrant's operations and financial condition;
- Whether the registrant has remediated or is currently remediating the incident; and
- Any changes in the registrant's policies and procedures as a result of the cybersecurity incident, and how the incident may have informed such changes.

Requirement to Disclose Cybersecurity Incidents That Have Become Material in the Aggregate. Registrants would also be required to disclose, to the extent known to management, when a series of previously undisclosed cybersecurity incidents that were individually immaterial have become material when viewed in the aggregate. If a determination is made that these incidents in the aggregate are material, registrants would need to disclose, in a periodic report for the period in which the determination is made:

- When the incidents were discovered and whether they are ongoing;
- A brief description of the nature and scope of such incidents;
- Whether any data was stolen or altered;
- The impact of such incidents on the registrant's operations and the registrant's actions; and
- Whether the registrant has remediated or is currently remediating the incidents.

The SEC notes that "while such incidents conceptually could take a variety of forms, an example would be where one malicious actor engages in a number of smaller but continuous cyber-attacks related in time and form against the same company and collectively, they are either quantitatively or qualitatively material, or both."[15]

Amendments to Form 10-K and Form 20-F Regarding Cybersecurity Policies and Governance. Proposed new Item 106 of Regulation S-K would also require extensive disclosure in Annual Reports on Form 10-K (and on Form 20-F for foreign private issuers) of cybersecurity risk management, strategy and governance, including:

- ***Policies and procedures for identifying and managing cybersecurity risks.*** Disclosure would be required, to the extent applicable, as to whether a registrant has: (i) a cybersecurity risk assessment program; (ii) engaged consultants, auditors or other third parties in connection with its cybersecurity program; (iii) policies and procedures relating to cybersecurity risks associated with use of third party service providers; (iv) business continuity, contingency and recovery plans in the event of a cybersecurity incident; and (v) modified its cybersecurity governance, policies and procedures or technologies as a result of previous cybersecurity incidents. Disclosure would also be required as to whether cybersecurity risks have affected or are reasonably likely to affect the registrant's results of operations or financial condition and whether such risks are considered as part of the registrant's business strategy, financial planning and capital allocation.
- ***The board of directors' role in cyber governance.*** Proposed Item 106(c) would require disclosure regarding the board's oversight of cybersecurity risk, including (i) whether the entire board, specific board members or a board committee is responsible for the oversight of cybersecurity risks; (ii) the processes by which the board is informed about cybersecurity risks, and the frequency of its discussions on this topic; and (iii) whether and how the board or board committee considers cybersecurity risks as part of its business strategy, risk management and financial oversight.
- ***Management's role in cyber governance.*** Proposed Item 106(c) would require disclosure of management's expertise in managing cybersecurity risks and implementing related policies, procedures and strategies, including:
  - Whether certain management positions or committees are responsible for measuring and managing cybersecurity risk, specifically the prevention, mitigation, detection, and remediation of cybersecurity incidents, and the relevant expertise of such persons or members;
  - Whether the registrant has designated a chief information security officer, or someone in a comparable position, and if so, to whom that individual reports within the registrant's organizational chart, and the relevant expertise of any such persons;
  - The processes by which such persons or committees are informed about and monitor the prevention, mitigation, detection and remediation of cybersecurity incidents; and
  - Whether and how frequently such persons or committees report to the board of directors or a committee of the board of directors on cybersecurity risk.
- ***Cyber expertise of any member of the board of directors.*** Proposed Item 407(j) would require registrants to disclose, in proxy statements and Annual Reports on Form 10-K, whether any member of the board of directors has cybersecurity expertise and, if so, the director's name and details sufficient to fully describe the nature of the expertise. An equivalent requirement would apply to foreign private issuers in Annual Reports on Form 20-F. Notably, proposed Item 407(j) would not define "cybersecurity expertise," but would include the following non-exclusive list of criteria to be considered in determining whether a director has expertise in cybersecurity:
  - Whether the director has prior work experience in cybersecurity;
  - Whether the director has obtained a certification or degree in cybersecurity; and
  - Whether the director has knowledge, skills or other background in cybersecurity.

  Proposed Item 407(j) would include a safe harbor, consistent with the safe harbor that applies to directors identified as audit committee financial experts, that the designation does not impose any greater duties, obligation or liabilities on any director identified as having cybersecurity expertise. Conversely, the identification of a cybersecurity expert on the board would not decrease the duties and obligations or liability of other board members.

Foreign Private Issuers. In addition to subjecting foreign private issuers to the same annual report disclosure requirements, the Proposed Rules would amend Form 6-K to add "cybersecurity incidents" as a reporting topic.[16]

iXBRL. Information disclosed under the Proposed Rules would be tagged using inline XBRL.

IMPLICATIONS

Although the Proposed Rules remain generally consistent with the principles-based approach that the SEC has historically taken on cybersecurity incident disclosures, they impose explicit timing and content requirements on cyber-related incident disclosures and add required disclosures of cybersecurity risk management, strategy and governance without regard to materiality. Although cybersecurity risks are critical to a range of companies, the detailed disclosures required by the Proposed Rules will not be material in all situations.

In addition, the proposed four-business-day window to disclose material cybersecurity incidents may raise challenges in a number of contexts. For example, a company undergoing a ransomware attack may be concerned that it could be exposed to heightened risks and harms that exceed the benefits of prompt disclosure if required to disclose the attack publicly while an intruder is still present in the company's network. In addition, as the facts and the company's understanding of the nature and impact of a cybersecurity incident quickly evolve, many companies will be challenged to identify and assess the materiality of a cybersecurity incident in order to report on a timely basis, and may need to update that disclosure as the incident evolves.

The four-business-day window may also be particularly challenging in connection with incidents involving unauthorized access to or disclosure of individuals' personally identifying information. It is not uncommon for a company in that circumstance to conclude that it has likely experienced a material incident, but needs additional time to determine the nature and magnitude of the information accessed. Under the Proposed Rules, disclosure of a breach affecting a large number of individuals may be required before the company can reasonably make the necessary determinations, and may lead to incoming questions and requests from potentially affected customers or other individuals that the company is not in a position to answer. That situation could expose the company to additional risks and reputational harm, without providing additional mitigation of risks or harms for affected individuals. In addition, the proposed four-business-day timeframe does not contemplate a reporting delay, including "when there is an ongoing internal or external investigation related to the cybersecurity incident."[17] As the SEC acknowledged in the Proposing Release,[18] the notification requirement may differ from existing obligations under state law or other federal regulations. These competing demands can obviously create a dilemma, and commenters would be well served by highlighting this dilemma (including the availability of deferred reporting if requested by law enforcement) in commenting on the Proposed Rules.

Therefore, if the Proposed Rules are adopted, companies should consult with legal advisors in order to navigate various state and federal requirements that may be implicated by additional disclosures on cybersecurity, especially as new state, federal and international laws concerning data privacy continue to proliferate, some of which provide private causes of action for data breaches.

The required disclosures contemplated by the Proposed Rules regarding the cybersecurity expertise of directors and management will likely intensify the pressure on companies—especially those with significant exposure to cybersecurity risks—to add "cyber experts" to their boards or C-suites. As widely reported, however, cybersecurity expertise at every level, including among boards and C-suites, is far exceeded by current demand in the United States. Accordingly, the required disclosures would intensify a demand that does not currently seem possible to meet. In addition, notwithstanding the proposed safe harbor from liability for the designated cybersecurity experts, this requirement could also intensify the scrutiny on the directors or executives that are identified as having that expertise, especially if a material cybersecurity incident occurs.

Registrants should also evaluate their existing cyber-incident reporting and cyber risk-assessment disclosure controls and procedures in light of the proposed requirement that companies disclose when a series of previous, immaterial cybersecurity incidents have become material when viewed in the aggregate. In particular, registrants may need to evaluate whether they have an appropriate framework in place that can identify patterns in cybersecurity incidents over time, and incorporate issues identified by front-line cybersecurity professionals into their disclosure controls and procedures. These actions by registrants will also serve other regulatory concerns presented by cybersecurity issues, as reflected by Chair Gensler's reference to the roles of the Department of Justice, the Federal Bureau of Investigation, and the Cybersecurity and Infrastructure Security Agency in his statement announcing the Proposed Rules.[19]

* * *

ENDNOTES

1 Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, SEC Release Nos. 33-11038; 34-943529; IC-34529 (March 9, 2022) (the "Proposing Release"). *See also*, SEC Fact Sheet: Public Company Cybersecurity; Proposed Rules (Mar. 9, 2022), *available at* https://www.sec.gov/files/33-11038-fact-sheet.pdf. The Proposed Rules were proposed by a 3 to 1 vote. In dissenting, Commissioner Peirce stated that the Proposed Rules "flirt[] with casting [the SEC] as the nation's cybersecurity command center, a role that Congress did not give us." She described her concerns that the proposed disclosure language would lead to "micromanagement" of "the composition functioning of boards" through the specific requirement disclosure requirements concerning the cybersecurity expertise of board members, for instance.

2 If adopted, the guidance set forth in both the 2011 Staff Guidance and the 2018 Interpretive Release would remain in place. Proposing Release at 16.

ENDNOTES (CONTINUED)

3 *See* SEC Charges Issuer with Misleading Investors About Cybersecurity Incident and for Inadequate Disclosure Controls, Sullivan & Cromwell Memo (Aug. 18, 2021), *available at* https://www.sullcrom.com/files/upload/sc-publication-SEC-brings-cybersecurity-charges-against-issuer.pdf; and SEC Sanctions Firms in Three Actions for Deficient Cybersecurity Controls, Sullivan & Cromwell Memo (Sept. 1, 2021), *available at* https://www.sullcrom.com/files/upload/SC-Publication-SEC-Sanctions-Firms-For-Deficient-Cybersecurity-Controls.pdf.

4 *See* SEC, In the Matter of Certain Cybersecurity-Related Events (HO-14225) FAQs, *available at* https://www.sec.gov/enforce/certain-cybersecurity-related-events-faqs.

5 Chair Gary Gensler, Speech on Cybersecurity and Securities Laws, Northwestern Pritzker School of Law's Annual Securities Regulation Institute (Jan. 24, 2022), *available at* https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124.

6 *Id.* at 11.

7 *Id.* at 12.

8 Executive Order on Improving the Nation's Cybersecurity, Exec. Order No. 14,028 (May 12, 2021), *available at* https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

9 *See* Press Release, Department of Homeland Security, DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators (May 27, 2021), *available at* https://www.dhs.gov/news/2021/05/27/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators; Press Release, Department of Homeland Security, DHS Announces New Cybersecurity Requirements for Surface Transportation Owners and Operators (Dec. 2, 2021), *available at* https://www.dhs.gov/news/2021/12/02/dhs-announces-new-cybersecurity-requirements-surface-transportation-owners-and.

10 In November 2021, the Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency (OCC) and the Federal Reserve Board of Governors jointly issued a final rule that requires banking organizations and service providers to notify their primary regulator within 36 hours after determining that a "cyber-security incident that rises to the level of a notification incident has occurred." Financial Institution Letter, Computer-Security Incident Notification Final Rule (Nov. 18, 2021), https://www.fdic.gov/news/financial-institution-letters/2021/fil21074.html. *See* Federal Banking Agencies Issue Final Rule Regarding Cyber Incident Notification Requirements (Nov. 22, 2021), *available at* https://www.sullcrom.com/files/upload/sc-publication-federal-banking-regulators-mandate-cybersecurity-incident-notification.pdf.

11 *See* OFAC Updates Ransomware Advisory, Sullivan & Cromwell Memo (Sept. 23, 2021), *available at* https://www.sullcrom.com/files/upload/SC-Publication-OFAC-Updates-Ransomeware-Advisory-Designates-Crypto-Exchange.pdf.

12 *See* FinCEN Updates Ransomware Advisory, Sullivan & Cromwell Memo (Nov. 11, 2021), *available at* https://www.sullcrom.com/files/upload/sc-publication-fincen-updates-advisory-regarding-reporting-ransomware-payments.pdf.

ENDNOTES (CONTINUED)

13 Strengthening American Cybersecurity Act, S. 3600, 117th Cong. (2022), *available at* https://www.congress.gov/bill/117th-congress/senate-bill/3600/text.

14 For purposes of the proposed Item 106, "cybersecurity incident means 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 means 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; and "information systems means 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." A "cybersecurity incident" is "to be construed broadly" and includes "an accidental exposure of data, a deliberate action or activity to gain unauthorized access to systems or to steal or alter data, or other system compromises or data breaches." Proposing Release at 42.

15 Proposing Release at 34.

16 As with all other Form 6-K disclosure items, the Proposed Rules note that foreign private issuers are only required to disclose on Form 6-K cybersecurity incidents that they are required to disclose elsewhere.

17 Proposing Release at 25.

18 *Id.* at 26.

19 Chair Gary Gensler, Statement on Proposal for Mandatory Cybersecurity Disclosures (Mar. 9, 2022), *available at* https://www.sec.gov/news/statement/gensler-cybersecurity-20220309.

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 875 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers or to any Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future publications by sending an e-mail to SCPublications@sullcrom.com.