Hogan Lovells

SEC Update

March 25, 2022

This is a commercial communication from Hogan Lovells. See note below.

SEC proposes significant new cybersecurity disclosure requirements

On March 9, 2022 the SEC proposed rule amendments that would require public companies to report detailed information about material cybersecurity incidents affecting their business and about their cybersecurity risk management and governance. The new requirements are intended to promote standardization of cybersecurity disclosure and the comparability of such disclosure across companies and time periods.

The SEC proposes to amend Regulation S-K and Exchange Act forms to require companies to report cybersecurity incidents on Form 8-K within four business days after the company determines the incident is material. Companies would also be required to provide updated disclosures on Forms 10-Q and 10-K about previously disclosed incidents, as well as to disclose in their periodic reports any series of previously undisclosed individually immaterial incidents that has become material in the aggregate.

The proposed requirements would extend beyond incident reporting to include information intended to enable investors to evaluate companies' ability to manage and mitigate their cybersecurity risk and exposure. Companies would be required to describe in their Form 10-K reports their policies and procedures for identifying and managing cybersecurity risk, including whether they consider cybersecurity risk as part of their business strategy, financial planning, and capital allocation.

The annual reporting requirements would also encompass disclosure about the board's oversight of cybersecurity risk, management's cybersecurity expertise, management's role in assessing and managing cybersecurity risk, and its role in implementing the company's cybersecurity policies, procedures, and strategies. In addition, companies would be obligated to disclose on Form 10-K and in their annual proxy statements whether any board member has cybersecurity expertise and, if so, to describe the nature of that expertise.

The SEC's release describing the proposed amendments (Release No. 33-11038) can be viewed here. The comment period on the proposal will be open until May 9.

Background

The SEC's rule proposal follows efforts by the Commission and its staff over the past decade to encourage enhanced disclosure of cybersecurity risks, incidents, and governance through interpretive guidance under the existing disclosure regime, which does not expressly refer to cybersecurity risks or incidents.

The Division of Corporation Finance published guidance in 2011 describing the application of specified items of Regulation S-K to cybersecurity risks and incidents and highlighting how the impacts of cybersecurity incidents can affect financial statement presentation. In an interpretive release published in 2018, in addition to revisiting the application of relevant disclosure topics, the Commission discussed how materiality assessments can shape the timing and content of cybersecurity disclosure. The SEC also addressed board oversight of cybersecurity risk, the importance of adequate disclosure controls and procedures, and the management of insider trading activity and Regulation FD compliance in this context. We discussed this guidance in the *SEC Updates* we issued in October 2011 and March 2018.

In recent years the SEC staff has reinforced this guidance by issuing numerous comment letters regarding cybersecurity disclosure as part of its filing review program. In addition, the SEC has brought enforcement actions against companies for disclosure control failures and misleading disclosures relating to cybersecurity incidents.

Notwithstanding the increased regulatory focus on cybersecurity disclosure, the SEC believes that cybersecurity risks and incidents are "underreported" and that the value of the published cybersecurity disclosure has been undermined by inconsistencies in timing, coverage, level of detail, and disclosure location. The SEC aims to address these purported deficiencies by adding to its rules a series of prescriptive requirements that are intended to provide a standardized framework for cybersecurity disclosure.

The SEC confirms in its release that companies should continue to consult the prior interpretive guidance for disclosure determinations and presentations that are not governed by the new requirements.

Proposed rules

Cybersecurity incident reporting

Current reporting on Form 8-K

The proposed amendments would add material cybersecurity incidents as a Form 8-K mandatory disclosure event under a new Item 1.05 to be captioned "Cybersecurity incidents."

To the extent known at the time of filing, the company would be required to disclose the following information about a material cybersecurity incident:

- when the incident was discovered;
- whether the incident is ongoing;
- a brief description of the incident's nature and scope;
- whether any data was stolen, altered, accessed, or used for any other unauthorized purpose;
- the incident's effect on the company's operations; and
- whether the company has remediated or is currently remediating the incident.

The SEC notes that, to mitigate the risk that prompt disclosure could subject a company to further harm, the company would not be expected to publicly disclose specific, technical information about its planned response, cybersecurity systems or related networks and devices, or potential system vulnerabilities in such detail as would impede its response or remediation. The company would be obligated to disclose in its future Form 10-Q or 10-K reports any material information about the incident that is not knowable or disclosable at the time of the Form 8-K filing.

The company would be required to file its Form 8-K within four business days after it determines that the cybersecurity incident it has experienced is material, rather than four business days after the date it discovers the incident. An instruction to Item 1.05 would direct the company to make a materiality determination "as soon as reasonably practicable after discovery of the incident." The SEC acknowledges that the company's management would be required "to make a rapid materiality decision" and expects that "in some cases" the company would make its materiality determination coincident with its discovery of the incident, while in other cases the company would not be able to make the materiality determination until a later date.

The SEC does not clarify the meaning of "discovery" in this context. As used in various U.S. federal and state breach notification statutes, the term may not necessarily mean the date on which an incident is first identified or detected.

Companies would not be permitted to delay disclosure beyond the Form 8-K deadline because of the existence of an ongoing internal or external investigation of the incident or because state law may allow later notification of the incident to regulators, consumers, or other parties. The filing deadline may create tension with managing notifications of the incident to other regulators, particularly under state breach notification laws that require notification "without unreasonable delay" or "as expeditiously as practicable," standards that historically have been understood to mean up to 30 days or longer after the incident discovery date. The SEC's proposal contains no exception for disclosure that would conflict with the company's other obligations under federal or state law, although the SEC has solicited comment on whether it should add such an exception to the final rule.

A "cybersecurity incident" potentially triggering Form 8-K reporting would be defined in a new Item 106 of Regulation S-K as "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." The SEC indicates that this definition "should be construed broadly" and provides the following non-exclusive list of cybersecurity incidents that could be disclosable under Item 1.05 if the company determines them to be material:

- an unauthorized incident – whether involving an accidental exposure of data or an attack to steal or alter data – that has compromised the

confidentiality, integrity, or availability of an information asset or violated the company's security policies or procedures;

- an unauthorized incident that has 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 stole 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.

The SEC's definition of cybersecurity incident is not the same as the definitions used by other regulatory bodies. As a result, occurrences that companies may not historically have classified as "incidents" may now be considered cybersecurity incidents for SEC disclosure purposes.

The SEC confirms that the materiality of a cybersecurity incident would be assessed consistently with existing materiality principles under the securities laws. Accordingly, a cybersecurity incident would be deemed material if there is a substantial likelihood that a reasonable stockholder would consider information about the incident important to an investment decision or if disclosure of the information would be viewed by a reasonable investor as having significantly altered the "total mix" of information made available. Echoing the materiality discussion in its 2018 guidance, the SEC emphasizes that this determination should take into account both qualitative and quantitative factors.

In recognition of the challenges inherent in making a rapid materiality determination, the proposed rules would provide that failure to report a cybersecurity incident on Form 8-K in a timely manner would not result in loss of the company's eligibility to file a short-form registration statement on Securities Act Form S-3, so long as Form 8-K reporting is current at the time the Form S-3 is filed. The rules would also add Item 1.05 to the list of Form 8-K items requiring rapid materiality determinations that are eligible for a limited safe harbor from liability under Exchange Act Section 10(b) and Rule 10b-5 thereunder if they are the subject of untimely filings.

Periodic reporting on Forms 10-Q and 10-K

The SEC proposes to adopt a new Item 106 of Regulation S-K, to be captioned "Cybersecurity," and to amend Forms 10-Q and 10-K to add requirements for cybersecurity incident reporting and other cybersecurity disclosures.

Item 106(d)(1) would require companies to disclose on Forms 10-Q and 10-K "any material changes, additions, or updates" to previous cybersecurity incident disclosures made pursuant to Item 1.05 of Form 8-K. The periodic disclosures would supply information about the incident not knowable or disclosable at the time of the Form 8-K filing or that reflect developments occurring during a subsequent reporting period. The SEC identifies the following types of potentially relevant disclosures:

- any material effect or potential future material impacts of the cybersecurity incident on the company's operations and financial condition;
- whether the incident has been or is being remediated; and
- any changes in the company's policies or procedures as a result of the incident, including how the incident may have informed the changes.

The SEC cautions that a development may require a company to "correct" its Item 1.05 disclosure by amendment rather than wait to disclose the new information in its next Form 10-Q or 10-K filing, if the Form 8-K disclosure becomes inaccurate or materially misleading as a result of the development. The SEC cites, as an example, a circumstance in which the impact of the cybersecurity incident is determined after the initial filing to be significantly more severe than previously disclosed.

Item 106(d)(2) would require cybersecurity disclosure in periodic reports similar to that prescribed by Item 1.05 of Form 8-K "to the extent known to management when a series of previously undisclosed individually immaterial cybersecurity incidents has become material in the aggregate." The SEC refers, as an example, to an instance where a "malicious actor engages in a number of smaller but continuous cyber-attacks related in time and form" that are collectively material. The company would be required to disclose the incidents in the periodic report for the period in which it determined that the incidents are material in the aggregate. The SEC has invited comment on whether a materiality determination related to a series of individually immaterial incidents should trigger a Form 8-K filing.

Cybersecurity governance reporting

The proposal also would amend Form 10-K to require companies to make governance-related disclosures required by Item 106 and by a new Item 407(j) of Regulation S-K. Companies also would be obligated to include the Item 407(j) disclosure in their annual proxy statements.

Risk management processes

New Item 106(b) would require companies to describe their policies and procedures, if any, for the identification and management of cybersecurity risks, which would include a discussion of the following:

- any cybersecurity risk assessment program and whether third parties are engaged as part of the program;
- policies and procedures to oversee and identify risks associated with third-party service providers;
- activities undertaken to prevent, detect, and minimize effects of cybersecurity incidents;
- whether the company has business continuity, contingency, and recovery plans in the event of a cybersecurity incident;
- whether cybersecurity incidents have informed changes in the company's governance, policies and procedures, or technologies;
- whether cybersecurity risks and incidents have affected or are reasonably likely to affect the company's results of operations or financial condition and, if so, how; and
- whether cybersecurity risks are considered as part of the company's business strategy, financial planning, and capital allocation and, if so, how.

The list of topics reflects the broad scope of the SEC's mandate for companies to provide meaningful information about their cybersecurity risk profile. In its release, the SEC highlights topics that would be appropriate for treatment in management's discussion and analysis of financial condition and results of operations, including disclosure about the financial impacts of previous cybersecurity incidents and discussion of cybersecurity threats as trends or uncertainties that would reasonably be likely to affect the company's future financial performance or position.

Board oversight of cybersecurity risk

Item 106(c)(1) would require companies to describe oversight of cybersecurity risk by the board of directors, including, as applicable:

- whether the entire board, specific directors, or a committee is responsible for oversight;
- the processes by which the board is informed of cybersecurity risks, and the frequency of its discussions on this topic; and
- whether and how the board considers cybersecurity risks in its business strategy, risk management, and financial oversight.

The SEC expects that this disclosure, along with the required disclosure about management's role in cybersecurity risk management described below, would better inform investors about how a company prepares for, prevents, or responds to cybersecurity incidents.

Management's role in cybersecurity

Item 106(c)(2) would require companies to describe management's role in cybersecurity risk assessment and management and in implementing the company's cybersecurity policies, procedures, and strategies, including:

- whether management positions or committees are responsible for measuring and managing risk, and the relevant expertise of such management personnel;
- whether there is a designated chief information security officer or someone serving in a comparable role, the position to which any such person reports within the company, 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 board committee on cybersecurity risk.

The SEC indicates that this disclosure should assist investors in understanding how companies are planning for cybersecurity risks and deciding how best to allocate their capital.

Board cybersecurity expertise

The SEC proposes to add a new paragraph (j) to Item 407 of Regulation S-K that would require companies to identify in their annual proxy statements which of their directors, if any, have cybersecurity expertise and to describe the nature of that expertise. The Item 407(j) disclosure also would appear in Form 10-K under Item 10 of Part III.

Item 407(j) would not define the experiences, skills, or tasks that constitute "cybersecurity expertise," but instead would include the following non-exclusive list of criteria a company could consider in determining whether a director has cybersecurity expertise:

- work experience in cybersecurity;
- a certification or degree in cybersecurity; or
- knowledge, skills, or other background in cybersecurity.

Although boards may have directors with oversight experience in cybersecurity matters, directors often lack the technical expertise associated with a number of the roles enumerated in Item 407(j). If the rule amendment is adopted, nominating committees can be expected to add cybersecurity expertise to the qualifications they consider in evaluating board composition and potential director candidates.

Structured data requirements for cybersecurity disclosure

To improve the accessibility and availability of cybersecurity disclosure, the proposal would require all disclosures under Item 1.05 of Form 8-K, Items 106 and 407(j) of Regulation S-K, and Item 16J of Form 20-F to be provided in Inline XBRL in accordance with Rule 405 of Regulation S-T and the EDGAR Filer Manual. The structured data requirement would include block text tagging of narrative disclosures and detail tagging of quantitative amounts. The SEC notes that this tagging would facilitate more efficient large-scale analysis and comparison of cybersecurity information across registrants and time periods, and better searchability of cybersecurity information.

Cybersecurity disclosure by foreign private issuers

The proposed rules would extend the requirements for enhanced cybersecurity incident and ongoing cybersecurity disclosures to foreign private issuers through amendments to Forms 6-K and 20-F.

To elicit timely cybersecurity incident disclosure, the proposal would amend Form 6-K to add "cybersecurity incident" to the reporting topics that may trigger a filing. Form 6-K requires disclosure of material information – including with respect to topics specified in the form – which the foreign private issuer makes or is required to make public under home jurisdiction law, files or is required to file under stock exchange rules, or distributes or is required to distribute to its security holders.

The proposal also would require periodic cybersecurity disclosures by foreign private issuers generally consistent with those required by domestic registrants. The SEC proposes to amend Form 20-F to add a new Item 16J which would require foreign private issuers to disclose annually material updates to previously disclosed cybersecurity incidents and cybersecurity governance information. Because Form 6-K would not require disclosure of all material cybersecurity incidents, but rather those otherwise required to be disclosed by the Form 6-K filing triggers noted above, new Item 16J(d)(2) would also require annual disclosure on Form 20-F of any previously undisclosed material cybersecurity incidents that occurred during the reporting period, including any series of previously undisclosed individually immaterial cybersecurity incidents that has become material in the aggregate.

Looking ahead

Consistent with the approach the SEC has taken in other recent rule proposals, the proposed amendments emphasize more rapid and detailed reporting and incorporate prescriptive requirements to promote uniform and comparable disclosures. As in the other recent proposals, the SEC also seeks to expand the scope of required disclosures to encompass a description of relevant governance policies and practices.

If adopted as proposed, the amended rules would increase the volume, frequency, and specificity of cybersecurity disclosures. Companies should consider whether they would need to augment their disclosure controls and procedures to ensure they are able, in a timely fashion, to identify cybersecurity incidents as defined by the SEC, evaluate their potential materiality, and prepare the enhanced disclosures called for under the proposed amendments. As part of this review, companies may find it necessary to revisit their incident response plans and processes, particularly regarding severity classifications and reporting escalation thresholds. Preparation for compliance with the new requirements also should include a critical reappraisal of existing cybersecurity risk management policies and related governance arrangements, which would be exposed to more intensive regulatory and investor scrutiny. In particular, in view of the proposed requirement to identify directors who have cybersecurity expertise, company boards may wish to adjust their nomination criteria to include this qualification.

Although the SEC underscores the expected benefits of enhanced disclosure to investors, it also recognizes the potential adverse impacts the new reporting requirements could have on companies. The proposed disclosure could potentially increase rather than decrease the vulnerability of public companies to cybersecurity incidents as a result of the insights the disclosures could give into a company's cybersecurity practices and readiness. The SEC acknowledges that, as a result of the additional disclosure, companies "may face increased risk" and "[m]alicious actors could engage in further attacks based on the information," in particular where an ongoing cyber-attack has not been resolved or where underlying security issues have not been remediated (and are disclosed as not having been remediated). The SEC further notes that malicious actors could gain new access to information about which companies lack cybersecurity expertise in the boardroom and robust risk management policies and procedures, which could allow such actors to "determine their targets accordingly."

As in any rulemaking, the final rules could differ in important respects from those proposed. The SEC has solicited comments on a range of alternative approaches to enhancing disclosure about cybersecurity incidents and related matters. Cybersecurity disclosure, like other measures proposed by the SEC over the last few months, is an area of focus for SEC Chair Gensler. Companies can expect the SEC to move quickly to adopt new disclosure requirements.

Contributors

Alan L. Dye (co-editor)
Partner, Washington, D.C.
Securities & Public Company Advisory
T +1 202 637 5737
alan.dye@hoganlovells.com

Richard Parrino (co-editor)
Partner, Washington, D.C.
Securities & Public Company Advisory
T +1 202 637 5530
richard.parrino@hoganlovells.com

John B. Beckman
Partner, Washington, D.C.
Securities & Public Company Advisory
T +1 202 637 5464
john.beckman@hoganlovells.com

Kevin K. Greenslade
Partner, Northern Virginia
Securities & Public Company Advisory
T +1 703 610 6189
kevin.greenslade@hoganlovells.com

William I. Intner
Partner, Baltimore
Securities & Public Company Advisory
T +1 410 659 2778
william.intner@hoganlovells.com

Paul Otto
Partner, Washington, D.C.
Privacy and Cybersecurity
T +1 202 637 5887
paul.otto@hoganlovells.com

Harriet Pearson
Senior Counsel, Washington, D.C., New York
Privacy and Cybersecurity
T +1 202 637 5477 (Washington, D.C.)
T +1 212 918 5548 (New York)
harriet.pearson@hoganlovells.com

J. Nicholas Hoover
Counsel, Baltimore
Securities & Public Company Advisory
T +1 410 659 2790
nick.hoover@hoganlovells.com

Additional contacts

Steven J. Abrams
Partner, Philadelphia
T +1 267 675 4671
steve.abrams@hoganlovells.com

Richard B. Aftanas
Partner, New York
T +1 212 918 3267
richard.aftanas@hoganlovells.com

Tifarah Roberts Allen
Partner, Washington, D.C.
T +1 202 637 5427
tifarah.allen@hoganlovells.com

C. Alex Bahn
Partner, Washington, D.C., Philadelphia
T +1 202 637 6832 (Washington, D.C.)
T +1 267 675 4619 (Philadelphia)
alex.bahn@hoganlovells.com

Jessica A. Bisignano
Partner, Philadelphia
T +1 267 675 4643
jessica.bisignano@hoganlovells.com

David W. Bonser
Partner, Washington, D.C.
T +1 202 637 5868
david.bonser@hoganlovells.com

Glenn C. Campbell
Partner, Baltimore, Washington, D.C.
T +1 410 659 2709 (Baltimore)
T +1 202 637 5622 (Washington, D.C.)
glenn.campbell@hoganlovells.com

David Crandall
Partner, Denver
T +1 303 454 2449
david.crandall@hoganlovells.com

John P. Duke
Partner, Philadelphia, New York
T +1 267 675 4616 (Philadelphia)
T +1 212 918 5616 (New York)
john.duke@hoganlovells.com

Allen Hicks
Partner, Washington, D.C.
T +1 202 637 6420
allen.hicks@hoganlovells.com

Paul Hilton
Partner, Denver, New York
T +1 303 454 2414 (Denver)
T +1 212 918 3514 (New York)
paul.hilton@hoganlovells.com

Eve N. Howard
Partner, Washington, D.C.
T +1 202 637 5627
eve.howard@hoganlovells.com

Bob Juelke
Partner, Philadelphia
T +1 267 675 4615
bob.juelke@hoganlovells.com

Paul D. Manca
Partner, Washington, D.C.
T +1 202 637 5821
paul.manca@hoganlovells.com

Michael E. McTiernan
Partner, Philadelphia
T +1 202 637 5684
michael.mctiernan@hoganlovells.com

Brian C. O'Fahey
Partner, Washington, D.C.
T +1 202 637 6541
brian.ofahey@hoganlovells.com

Tiffany Posil
Partner, Washington, D.C.
T +1 202 637 3663
tiffany.posil@hoganlovells.com

Leslie (Les) B. Reese, III
Partner, Washington, D.C.
T +1 202 637 5542
leslie.reese@hoganlovells.com

Richard Schaberg
Partner, Washington, D.C., New York
T +1 202 637 5671 (Washington, D.C.)
T +1 212 918 3000 (New York)
richard.schaberg@hoganlovells.com

Abigail C. Smith
Partner, Washington, D.C.
T +1 202 637 4880
abigail.smith@hoganlovells.com

Michael J. Silver
Partner, New York, Baltimore
T +1 212 918 8235 (New York)
T +1 410 659 2741 (Baltimore)
michael.silver@hoganlovells.com

Andrew S. Zahn
Partner, Washington, D.C.
T +1 202 637 3658
andrew.zahn@hoganlovells.com

Stephen M. Nicolai
Counsel, Philadelphia
T +1 267 675 4642
stephen.nicolai@hoganlovells.com

Alicante
Amsterdam
Baltimore
Beijing
Berlin**
Birmingham
Boston
Brussels
Budapest*
Colorado Springs
Denver
Dubai
Dublin
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta *
Johannesburg
London
Los Angeles
Louisville
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Moscow***
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
Riyadh*
Rome
San Francisco
São Paulo
Shanghai
Shanghai FTZ*
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar*
Warsaw
Washington, D.C.

*Our associated offices
**Legal Services Center
*** Progressing with a wind down of operations in Moscow

www.hoganlovells.com