SEC PROPOSES NEW DISCLOSURE OBLIGATIONS FOR PUBLIC COMPANIES RELATING TO CYBERSECURITY INCIDENTS

In the weeks leading up to the Russian invasion of Ukraine, cybersecurity experts (within and outside of government) warned of the increased threat of cyber threats. These warnings were hardly new, though more pointed, coming only a year after the compromise of the SolarWinds Orion software product. In fact, cybersecurity risks have increased significantly in recent years, due to the comprehensive shift to digitalization of operations, the increased prevalence of remote work, the ease with which increasingly sophisticated criminal elements (including those with the tacit or more direct support of malign state actors) can monetize cybersecurity attacks through ransomware, the deep and dark webs to sell stolen data, and the use of crypto-assets to hide the flow of money, and increased reliance by businesses on third-party service providers for IT services.

A survey conducted by EY in 2019 found that CEOs of the largest 200 global companies rated "national and corporate cybersecurity" as the most significant threat to business growth and the global economy in the next five to ten years. Boards and management teams are equally concerned, as are investors.

Cybersecurity incidents present a host of adverse consequences for businesses, ranging from costs incurred as a result of business interruption, to payments to meet ransomware demands, remediation costs, insurance premiums and other costs to protect IT infrastructure, lost revenue from theft or appropriation of proprietary information, litigation and legal risks, and damage to reputation and long-term shareholder value.

The SEC Takes Further Action

In light of the foregoing, and believing that investors and the markets would benefit from more timely, more consistent and more comprehensive disclosure about material cybersecurity incidents and the management of cybersecurity risks, the SEC has proposed amendments to existing rules as well as new rules to standardize disclosure by SEC reporting companies (domestic and foreign) regarding risk management, strategy, governance and incident reporting relating to cybersecurity. These actions were foreshadowed, as I noted in an earlier briefing in January, by SEC enforcement action and public statements from the SEC.

Specifically, today's proposal would require:

- Current reporting (on Form 8-K, pursuant to proposed new Item 1.05) about material cybersecurity incidents, within four business days after a registrant has determined it has experienced a material cybersecurity incident (rather than four business days after the date the incident is discovered), to include, to the extent known at the time the Form 8-K is filed:
    - 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.
- Periodic disclosure (set forth in proposed new Item 106 of Regulation S-K/Item 16J of Form 20-F) in respect of, among other things:
    - company policies and procedures to identify and manage cybersecurity risks; and
    - management's role, and relevant expertise, in assessing and managing cybersecurity-related risks and in implementing cybersecurity policies, procedures and strategies.
- Periodic disclosure (set forth in proposed Item 407(j) of Regulation S-K and amendments to Form 20-F) of the expertise, if any, of members of the board of directors and the board's role in overseeing cybersecurity risk, including
    - whether the entire board, or a committee, is responsible for oversight of cybersecurity risks;
    - the process by which the board is informed about such risks and the frequency of discussion on this topic; and
    - whether and how the board/committee considers cybersecurity risk as part of business strategy, risk management and financial oversight.
- Updated disclosure of previously reported material cybersecurity incidents and, to the extent known to management, of previously undisclosed individual immaterial cybersecurity incidents that are determined to have become material in the aggregate (pursuant to proposed new Item 106(d) of Regulation S-K/Item 16J(d) of Form 20-F), which would be set forth in Form 10-K or 10-Q reports for domestic registrants (on a quarterly basis) or in Form 20-F for foreign private issuers (on an annual basis)
- Preparation of the foregoing in Inline XBRL.

Background

These proposals build largely on existing guidance, including the Division of Corporation Finance's interpretive guidance on cybersecurity risks and incidents issued in 2011 (CF Disclosure Guidance: Topic No. 2) and the SEC's guidance issued in 2018 (Commission Statement and Guidance on Public Company Cybersecurity Disclosures). The 2018 guidance had identified the following existing provisions of Regulation S-K that could require disclosure about cybersecurity risks, governance and incidents: Item 105 (Risk Factors), Item 303 (MD&A), Item 101 (Business Description), Item 103 (Legal Proceedings) and Item 407 (Corporate Governance). The 2018 guidance also identified Regulation S-X as potentially applicable as well, and highlighted the importance of disclosure controls and procedures in the context of cybersecurity risks, the potential applicability of Regulation FD and the importance of adherence to securities trading policies in light of possible incidents and cyber vulnerabilities.

For purposes of the proposed rules,

- "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. An incident could include 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.

- "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.

Just last month, the SEC proposed new rules and rule amendments for investment advisers and investment funds relating to policies and procedures to address cybersecurity risks, as well as reporting of, and recordkeeping for, cybersecurity incidents.

Further Detail on Proposed Incident Disclosure (Item 1.05)

The proposing release notes that notwithstanding the existing guidance, current reporting about cybersecurity incidents may contain insufficient detail, may be difficult to locate, may not be timely and may be inconsistent. The proposals are intended to remedy the perceived deficiencies. Because the Form 8-K disclosure is tied to the date a registrant determines an incident is material, Instruction 1 to proposed Item 1.05 provides that registrants "shall make a materiality determination regarding a cybersecurity incident as soon as reasonably practicable after discovery of the incident."

Registrants are directed to the seminal cases on materiality (including cases addressing probability and magnitude). This generally would call for "an assessment in light of the specific circumstances presented by applying a well-reasoned, objective approach from a reasonable investor's perspective based on the total mix of information."

The SEC has provided the following non-exclusive list of examples of cybersecurity incidents that may trigger disclosure under proposed Item 1.05:

- 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 or 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 other 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 data that was stolen or altered.

The proposing release notes that proposed Item 1.05 would not provide for a reporting delay when there is an ongoing internal or external investigation related to the cybersecurity incident. The release cites the 2018 guidance to the effect that, while an ongoing

investigation might affect the specifics in the registrant's disclosure, "an ongoing internal or external investigation – which often can be lengthy – would not on its own provide a basis for avoiding disclosures of a material cybersecurity incident." The proposing release also notes that, to the extent proposed Item 1.05 would require disclosure in a situation in which a state law delay provision would excuse notification, the registrant nonetheless might be required to disclose the incident pursuant to Item 1.05 even though it would be entitled to delay incident reporting under a particular state law.

The SEC proposes to amend Form 6-K to include material cybersecurity incidents as triggering events for reporting purposes.

The SEC proposes to amend Forms S-3 and SF-3 to provide that untimely filing of Form 8-K by reason of an Item 1.05 incident would not result in the loss of form eligibility. It also proposes that Item 1.05 disclosure would be subject to the limited safe harbor from Section 10(b) and Rule 10b-5 liability under amended Rules 13a-11(c) and 15d-11(c).

Further Detail on Updates of Previous Incidents (Proposed Item 106(d)(1))

The short time frame for incidence reporting almost guarantees that updates will be required, whether material changes to, additions to or simply updates of prior disclosure. It might well be the case that regular updates for some period of time are required. Disclosure would be required in the periodic report (on Form 10-K, Form 20-F or Form 10-Q) for the period in which the change, addition or update occurs.

Proposed Item 1.06(d)(1) provides the following non-exclusive examples of triggers for updated disclosure:

- 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;
- where 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 incident, and how the incident may have informed such changes.

Further Detail on Disclosure of Incidents that Become Material in the Aggregate (Proposed Item 106(d)(2))

Proposed Item 1.06(d)(2), in effect, would require registrants to assess the materiality of cybersecurity incidents on an individual and on an aggregate basis. If individual incidents are determined to be material in the aggregate, disclosure would be required as to: 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. Disclosure would be required in the periodic report for the period in which the determination is made that previous individual immaterial incidents are in the aggregate material.

Further Detail on Disclosure of Risk Management and Strategy (Proposed Item 106(b))

The proposing release notes that disclosure of incidents tends not to be accompanied by disclosure of risk oversight and related policies and procedures or as to the impact on strategy, financial outlook and planning. Proposed Item 106(b) is intended to remedy these perceived deficiencies. Disclosure regarding policies and procedures would extend to selection and oversight of third-party service providers.

Proposed Item 106(b) would require disclosure, as applicable, of whether

- the registrant has a cybersecurity risk assessment program, and if so, it must provide a description of such program;
- the registrant engages assessors, consultants, auditors or other third parties in connection with any cybersecurity risk assessment program;
- the registrant has policies and procedures to oversee and identify the cybersecurity risks associated with its use of any third-party service provider (including, but not limited to, those providers that have access to the registrant's customer and employee data), including whether and how cybersecurity considerations affect the selection and oversight of these providers and contractual and other mechanisms the registrant uses to mitigate cybersecurity risks related to these providers;
- the registrant undertakes activities to prevent, detect and minimize effects of cybersecurity incidents;
- the registrant has business continuity, contingency and recovery plans in the event of a cybersecurity incident;
- previous cybersecurity incidents have informed changes in the registrant's governance, policies and procedures, or technologies;
- cybersecurity related risk and incidents have affected or are reasonably likely to affect the registrant's results of operations or financial condition, and if so, how; and
- cybersecurity risks are considered as part of the registrant's business strategy, financial planning and capital allocation, and if so, how.

Further Detail on Disclosure of Cybersecurity Governance (Proposed Item 106(c))

Proposed Item 106(c)(1) would require disclosure of a registrant's cybersecurity governance, including the board's oversight of cybersecurity risk and a description of management's role in assessing and managing cybersecurity risks, the relevant expertise of such management, and its role in implementing the registrant's cybersecurity policies, procedures and strategies. This would include, as applicable, disclosure of:

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

As for management's role, proposed Item 106(c)(2) would require disclosure, among other things, of:

- 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 organization, 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 or a committee of the board on cybersecurity risk.

Further Detail on Board Expertise (Proposed Item 407(j))

The proposed amendments to Item 407 would require disclosure about the cybersecurity expertise of members of the board, if any. If any board member has cybersecurity expertise, the registrant would have to disclose the name(s) of any such director(s), and provide such detail as necessary to fully describe the nature of the expertise.

Proposed Item 407(j) would not define what constitutes "cybersecurity expertise," since such expertise may cover different experiences, skills and tasks. Proposed Item 407(j)(1)(ii) does, however, include the following non-exclusive list of criteria that a registrant should consider in reaching a determination on whether a director has cybersecurity expertise:

- whether the director has prior work experience in cybersecurity, including, for example, prior experience as an information security officer, security policy analyst, security auditor, security architect or engineer, security operations or incident response manager, or business continuity planner;
- whether the director has obtained a certification or degree in cybersecurity; and
- whether the director has knowledge, skills or other background in cybersecurity, including, for example, in the areas of security policy and governance, risk management, security assessment, control evaluation, security architecture and engineering, security operations, incident handling or business continuity planning.

An "expert" for this purpose would not trigger expert status for any other purpose, including for purposes of Section 11 of the Securities Act.

Further Detail for Foreign Private Issuers

The SEC proposes to amend Form 20-F (for annual reports only) to add Item 16J to require foreign private issuers to include in their annual reports on Form 20-F the same type of disclosure proposed in Items 106 and 407(j). Guidance is provided for foreign private issuers to address different board structures for purposes of Items 106(c) and 407(j).

With respect to incident disclosure, where a foreign private issuer has previously reported an incident on Form 6-K, the proposed amendments would require an update regarding such

incident, consistent with proposed Item 106(d)(1). Form 20-F would be amended to require disclosure on an annual basis of information regarding any previously undisclosed material cybersecurity incidents that have occurred during the reporting period, including a series of previously undisclosed individually immaterial cybersecurity incidents that have become material in the aggregate.

Incidentally, if the SEC has in mind placing domestic registrants and foreign private issuers on equal footing when it comes to incidence reporting, there is an interpretative question for foreign private issuer disclosure, as Form 6-K disclosure needs a predicate: disclosure required locally, disclosure made pursuant to stock exchange requirements or disclosure otherwise distributed to shareholders. It is not automatic, while Form 8-K is.

Concluding Thoughts

While it is hard to take issue with the need for timely, uniform and comprehensive disclosure of cybersecurity matters, the technical complexity of information systems that could be compromised and/or the need to react in real time to what might be an existential threat to a business (for example, in the context of a ransomware attack) could make incidence reporting a fraught proposition.

There undoubtedly will be operational issues raised in the comment process.

- Is the customary 8-K reporting cycle too short for these incidents?
- Could disclosure harm efforts to resolve an ongoing attack?
- Are there potential national security implications of real time reporting?
- How quickly can registrants react when the incident involves a third-party service provider?
- Could SEC requirements potentially conflict with obligations of foreign private issuers in their home jurisdictions?

No doubt, there will be more.

* * * *

Mark S. Bergman
7Pillars Global Insights, LLC
Washington, D.C.
March 9, 2022