protiviti®
Global Business Consulting

SEC Cybersecurity Disclosure Enhancements: Efforts to Boost Investor Confidence

August 2, 2023

On July 26, 2023, the U.S. Securities and Exchange Commission (SEC) adopted amendments[1] to its rules on cybersecurity risk management, strategy, governance and incident reporting by public companies subject to the reporting requirements of the Securities Exchange Act of 1934. The SEC's view is that cybersecurity threats and incidents pose an ongoing risk to public companies, investors and market participants, as evidenced by the growing number and greater frequency of occurrences of attacks being launched by cyber criminals who are using increasingly sophisticated methods.

The amendments are intended to provide investors with greater information and transparency about cybersecurity risks and threats, a company's ability to identify and manage threats, and oversight and governance provided by senior leadership and the board of directors. The objective of the amendments is to allow investors to better manage risk in their portfolio, as cybersecurity incidents can have potentially significant impacts on a company's operations and performance.

Overview

The adopted amendments increase reporting and disclosure requirements for companies registered with the SEC. The new requirements can be summarized as follows:

Key Definitions

As a result of commentary received since its March 2022 proposed rules, the SEC has adjusted the original language of the amendments to include some key terms. Understanding the meaning of these final key terms will be important as companies determine what to disclose.

- **Materiality**: The SEC has emphasized the concept of materiality for many of the requirements. For purposes of the amendments, "materiality" would be evaluated consistent with precedents set forth in judicial decisions; e.g., information is material

[1] "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure," U.S. Securities and Exchange Commission, July 31, 2023, available at www.sec.gov/files/rules/final/2023/33-11216.pdf.

if "there is a substantial likelihood that a reasonable shareholder would consider it important" in making an investment decision or if it would have "significantly altered the 'total mix' of information available." Furthermore, "doubts as to the critical nature" of the relevant information should be "resolved in favor of [investors]."[2] Evaluating materiality entails consideration of both quantitative and qualitative factors, e.g., the historical or prospective financial condition or operations of the company, company reputation and brand image, customer or vendor relationships, as well as compliance with regulations, among other things. The analysis should address both the immediate fallout and any longer-term effects, considering all facts and circumstances.

- **Cybersecurity incident**: The SEC's definition used is mostly aligned with definitions of a cybersecurity incident, as articulated by NIST SP 800-137 and the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). All three definitions focus on the confidentiality, integrity and availability of information systems. The SEC's definition specifically states that a cybersecurity incident is "an unauthorized occurrence, or a series of related occurrences on or conducted through a registrant's information systems, that jeopardizes the confidentiality, integrity or availability of [its] information systems or any information residing therein." The SEC's deviation from the proposing release is to include as part of the definition "a series of related unauthorized occurrences." In addition, in response to comments, the Commission dropped the requirement to disclose "a series of previously undisclosed individually immaterial cybersecurity incidents become material in the aggregate."

Reporting of Cybersecurity Incidents

The focus of reporting of cybersecurity incidents shifted slightly from the March 2022 proposed release. Reporting should examine the impacts of a material cybersecurity incident and does not require reporting of details of the incident. Important aspects of reporting include the following:

- Reporting should focus on the nature, scope and timing of any incident determined to be material and its impact or reasonably likely impacts.

[2] TSC Industries, Inc. v. Northway, Inc. 426 U.S. 438 (1976).

- Reporting should be on Form 8-K (or Form 6-K for Foreign Private Issuers) no later than four business days after it is determined that the incident has had or could have a material impact.
- Reporting should include cybersecurity incidents that occur at third-party service providers or vendors if the impact of those incidents would be considered material.
- If impacts or facts about the cybersecurity incident change, companies can update their reporting by filing an updated Form 8-K/6-K or through periodic reporting (10-Q or 10-K).

Describe Risk Management Processes

Amendments to Regulation S-K were initially proposed because the SEC found that many companies that have previously disclosed a cybersecurity incident did not provide sufficient information about their cybersecurity risk oversight or processes. With the new amendments, the SEC is taking a more prescriptive approach to requiring companies to describe their processes for identifying, assessing and managing material cybersecurity risks and threats. Specific requirements include:

- A high-level description of cybersecurity risk management functions, including how risks are identified and the processes used to assess the risk level and management practices to assure risks are reduced to and maintained at a reasonable level;
- Insight into how the cybersecurity risk management functions have been integrated into broader risk management systems and processes – for instance, risk reporting and monitoring processes used in conjunction with the enterprise risk management process;
- Disclosure of whether assessors, consultants, auditors and other third parties are engaged by the issuer to assist with its cybersecurity risk management functions and processes;
- A description of the processes used to oversee and identify cybersecurity risks associated with using third-party service providers; and
- Whether any risks from cybersecurity threats, including those associated with previous incidents, have materially impacted or are reasonably likely to materially impact the company's business strategy, operations or financial condition and, if so, how.

Disclosure of the Board's and Management's Governance Role

The amendments to Regulation S-K also include new requirements relating to governance. The board of directors' oversight and management's role in assessing and managing cybersecurity risks must be disclosed. Key aspects of this disclosure include:

- The board committee or subcommittee responsible for overseeing risks from cybersecurity threats;
- The processes by which the board or its designated committee is informed about cybersecurity risks, e.g., the frequency in which the board is provided information and the role and responsibilities of the board in overseeing cybersecurity risks;
- The management position(s) or committee(s) responsible for assessing and managing cybersecurity risks, including the relevant expertise of the individuals involved in these capacities;
- The processes by which management or its committees are informed about and monitor the prevention, detection, mitigation and remediation of cybersecurity incidents; and
- Whether management reports information regarding cybersecurity risks to the board or its designated committees.

Note that the SEC elected to strike the required disclosure in the proposing release pertaining to the cybersecurity expertise of board members. Many commenters pointed to the limited talent pool for such expertise and that smaller companies would be at a disadvantage due to limited resources.

Foreign Private Issuers

The amendments recognized that investors will need similar information about cybersecurity practices and incidents from Foreign Private Issuers. The amendment made it clear that Foreign Private Issuers should provide this information through Form 6-K and Form 20-F filings.

Timeline for Implementation

The amendments set forth the following effective dates:

December 15, 2023	10-K and 20-F disclosures start for companies filing on or after this date
December 18, 2023, or 90 days after the Federal Register publication date, whichever is later	8-K and 6-K disclosures start on this date
June 15, 2024, or 270 days after the Federal Register publication date, whichever is later	For "smaller reporting companies," 8-K and 6-K disclosures start on this date

These effective dates are, for the SEC, unusually immediate, with an "on or after" date for filings that brings this year's annual reports, and other required periodic reports, into play. Note that organizations falling into the "smaller reporting company" category are being granted an extra 180 days before they need to comply with the rules outlined in Forms 8-K or 6-K. However, these companies must meet the December reporting requirements for their 10-K and 20-F disclosures. Generally, a company qualifies as a "smaller reporting company" if its public float is less than $250 million, or if it has less than $100 million in annual revenues and either no public float or a public float of less than $700 million.

Preparing for Change – Some Points to Consider

In preparing for compliance, issuers should begin familiarizing the appropriate business leaders with the new requirements. At a minimum, organizations should include their cybersecurity, legal, privacy and compliance teams in these initial discussions.

One of the first areas to consider will be the new regulation's near-term timelines. Depending on the company's fiscal year end, the annual reporting requirements (via 10-K and 20-F disclosures) and any incident reporting (via 8-K and 6-K disclosures) begin in or after December 2023. As issuers prepare for these key dates, they should understand and formulate the depth and scope of the narrative they choose to articulate for these various filings.

During the preparatory process, we encourage organizations to review their incident response plans and start by ensuring they are aligned with the following key definitions highlighted by the SEC. Achieving alignment on this front could have a profound impact on when and how an incident response plan is activated.

- **Cybersecurity incident** is an unauthorized occurrence, or a series of related unauthorized occurrences, on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity or availability of the registrant's information systems or any information residing therein.
- A **cybersecurity threat** is any potential unauthorized occurrence on or conducted through a registrant's information systems that may result in adverse effects on the confidentiality, integrity or availability of the registrant's information systems or any information residing therein.
- **Information systems** refer to electronic 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 its operations.

Of particular concern for organizations is the window of four business days for reporting incidents. The four-business-day requirement for public companies to provide Form 8-K filings typically relates to the transactions and events for which registrants have advance notice and time to prepare draft disclosures well in advance. For this regulation, however, the window begins once an unexpected incident is evaluated to be material in nature. Therefore, organizations need to ensure they have a firm grasp of the process by which they will identify and escalate incidents and define materiality once the crucial moment occurs, as the SEC's amendment requires a determination "without unreasonable delay." As this process entails gathering the necessary information relating to the nature, scope and timing of the incident and bringing to bear the judgment of the appropriate parties, it makes sense to plan in advance how it will function, the criteria it considers and who serves as point. Additionally, the appropriate data will need to be captured in an ongoing manner as the need could arise to provide ongoing updates via Form 8-K/6-K or other planned periodic filings. These points should be incorporated into the incident response plan.

Although materiality may be a "moving target" for many organizations, the reality is that the SEC decided not to carve out a cybersecurity-specific threshold, as doing so would be a significant departure from its policies on the subject. Accordingly, the Commission reverted to the longstanding standard set out in the cases addressing materiality in the securities laws, e.g., the "reasonable investor" test. This makes the determination a legal question, strongly pointing toward the need to involve legal counsel in the decision-making process

when determining materiality. Certainly, an analysis of known trends or uncertainties that result in, or could likely result in, a change to an organization's liquidity or financial position, a change in the mix and relative cost of its capital resources, or an adverse impact on revenues or income from continuing operations would have a bearing in the determination.

In some cases, incidents could pose a substantial risk to national security or public safety (as determined by the U.S. Attorney General). In these cases, a Form 8-K/6-K disclosure delay may be granted (for 30 to 60 days, depending on the circumstances) upon notifying the Commission in writing. The potential for such situations suggests that organizations have as part of their incident response plans a provision for notifying and coordinating with relevant federal law enforcement agencies, as circumstances dictate.

Third parties continue to have an expanding role within key business processes across all industries. This topic generated a lot of feedback to the SEC from commenters. While the regulation acknowledges the role and impact of third-party providers, the final rule ultimately landed in a gray area. The SEC specifically stated that "we are not exempting registrants from providing disclosures regarding cybersecurity incidents on third-party systems they use, nor are we providing a safe harbor for information disclosed about third-party systems."

Depending on the circumstances of an incident that occurs on a third-party system, disclosure may be required by both the service provider and its customer, or by one but not the other, or by neither. This will be a challenge, as companies generally have reduced visibility into third-party systems they do not control. The good news is that the final rule concedes these challenges exist by stipulating that registrants should disclose third-party systems issues based on the information known or reasonably available to them and is consistent with the Commission's general rules regarding the disclosure of information that is difficult to obtain.

To that end, the final rules generally do not require that registrants conduct additional inquiries outside of their regular channels of communication with third-party service providers pursuant to their contractual obligations and rights and in accordance with the registrants' disclosure controls and procedures. The bottom line: Organizations need to be aware of the importance third parties play in their business operations and should be ready to respond to investor questions if an incident that originates at a third party has a material impact on their operations. It also may be smart to include a provision in service contracts

specifying the third party's disclosure obligations to the registrant and ensure the appropriate consideration and evaluation of use of third parties and third-party risk as a component of the organization's overall cybersecurity risk posture.

In determining the proper level of detail to provide about the cybersecurity program in Forms 10-k and 20-F – specifically focusing on risk management, strategy and governance – a good starting point may be the issuer's environmental, social and governance (ESG) report. Some organizations already have outlined their cybersecurity and privacy programs in that report. Alternatively, it may be useful to review the ESG reports and past cybersecurity disclosures of other organizations in the industry to ascertain how much detail they are using to describe their programs.

Preparing for Change – If Starting from Scratch

For companies starting from scratch, following is a template with a number of important questions to address:

- What processes, if any, exist for assessing, identifying and managing material risks from cybersecurity threats?
  - Are these processes described in sufficient detail so that a reasonable investor would understand them?
  - Are processes in place to oversee and identify material risks from cybersecurity threats associated with any third-party service provider(s)?
  - How have the described cybersecurity processes been integrated into the overall risk management system or processes?
  - Is the company leveraging assessors, consultants, auditors or other third parties in connection with its processes?
- Have any risks from cybersecurity threats, including any previous cybersecurity incidents, materially affected (or are reasonably likely to materially affect) the company's business strategy, results of operations or financial condition? If so, how?
  - Are cybersecurity risks considered as part of the registrant's strategy-setting, financial planning and capital allocation processes? If so, how?

  - What is management's role in assessing and managing the material risks from cybersecurity threats?

- How does the board oversee risks from cybersecurity threats?
  - Is there a board committee or subcommittee responsible for such oversight?
  - What is the process by which the board or designated committee is informed about these risks?
- Which management positions or committees are responsible for assessing and managing cybersecurity risks?
  - What is the nature of the relevant expertise of these parties?
  - What are the processes by which such persons or committees are informed about, and are able to monitor, the prevention, detection, mitigation and remediation of cybersecurity incidents?
  - How do such persons or committees report information about cybersecurity risks to the board of directors or its designated committee?

In Summary

In adopting these amendments, the SEC attempted to find common ground that avoids risking company security and protects investors' interests. But its prescriptive approach is not without controversy. As one of the two dissenting SEC commissioners stated, the final rules "impose a prescriptive disclosure regime" on the Commission's February 2018 interpretive release discussing how companies should consider the materiality of cybersecurity risks and incidents when preparing their filings under the securities laws. In his words, the amendments "swing a hammer at the current regime and create new disclosure obligations for cybersecurity matters that do not exist for any other topic."[3]

[3] "Statement on the Final Rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure," Commissioner Mark T. Uyeda, July 26, 2023, available at www.sec.gov/news/statement/uyeda-statement-cybersecurity-072623.

That said, the SEC's amendments to rules on cybersecurity risk management, strategy, governance and incident reporting by public companies subject to the reporting requirements of the Securities Exchange Act of 1934 are intended to help assure both timely and consistent information about cybersecurity risks and incidents. Their importance is underscored by the significant and increasing amount of the world's economic activities occurring through digital technology and electronic communications. Investors and other capital market participants depend on companies' use of secure and reliable information systems and data to conduct their businesses. With the ever-evolving threat landscape, cybersecurity continues to attract investor interest and regulatory scrutiny. That scrutiny will be directed not only toward public companies, but also toward those companies seeking to go public and those being acquired by public companies. Time will tell if these new disclosures serve their interests.

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, digital, legal, HR, governance, risk and internal audit through our network of more than 85 offices in over 25 countries.

Named to the 2023 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 80 percent of Fortune 100 and nearly 80 percent of Fortune 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

protiviti®