protiviti®
Global Business Consulting

SEC Cybersecurity Disclosure Enhancements: They're Coming, in One Form or Another

May 8,
2023

In March of 2022, the U.S. Securities and Exchange Commission (SEC) proposed amendments 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 threat to public companies, investors, and market participants, as evidenced by the growing number and greater frequency of occurrences of cyber attacks being launched by cyber criminals who are using increasingly sophisticated methods.

The official comment period on the proposal ended on May 9, 2022, with some 139 comment letters from companies, law firms, associations and other stakeholders were received. Since the end of the comment period 41 additional parties have provided additional considerations and comments regarding the proposed rules. The initial expectation for the final rules to be published in April of 2023 has passed and we do expect that the rules will be made final in the near future.

The SEC proposal: An overview

The proposed amendments[1] would require, among other things:

- Reporting of a cybersecurity incident within *four business days* after the registrant determines that it has experienced a material cybersecurity incident. (Note: For purposes of the proposed cybersecurity incidents disclosure, "materiality" would be evaluated consistent with precedents set forth in judicial decisions, e.g., information is material 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."

[1] "SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies," U.S. Securities and Exchange Commission, March 9, 2022, available at www.sec.gov/news/press-release/2022-39.

- Reporting of material cybersecurity incidents and periodic reporting to provide updates about previously reported cybersecurity incidents, including any material impact on the issuer's current and future 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 incident.
- Reporting of cybersecurity incidents that have become material in the aggregate.
- Disclosure of the company's policies and procedures to identify and manage cybersecurity risks; the extent to which it engages third parties in its cyber risk assessment program; policies and procedures to oversee and identify cybersecurity risks associated with its use of third-party service providers; the business continuity, contingency and recovery plans in place; and how cybersecurity risks are considered as part of the registrant's business strategy, financial planning and capital allocation.
- Disclosure of the issuer's board of directors' oversight of cybersecurity risk, and management's role and expertise in assessing and managing cybersecurity risk and implementing cybersecurity policies and procedures.
- Annual reporting or certain proxy disclosures about whether any member of the board of directors possesses cybersecurity expertise.

The intent of these proposed amendments is to inform investors better about a registrant's risk management, strategy and governance and to provide timely notification of material cybersecurity incidents. The amendments also apply to foreign private issuers and add "cybersecurity incidents" as a reporting topic.

Support from powerful quarters exists

The day after the comment period ended, the seven senators cosponsoring the Cybersecurity Disclosure Act (S. 808) released a letter[2] encouraging the SEC to issue the proposal in its present form. The letter notes that the proposal follows the intent of the cosponsored legislation to encourage directors to play a more effective role in cybersecurity oversight at the public companies they serve. The senators' motivation is their assertion that cybersecurity incidents have never been more frequent, complex and costly.

[2] "Leading U.S. Senators Urge SEC to Finalize Tough Cybersecurity Disclosure Rules for Public Companies," May 10, 2022, available at www.warner.senate.gov/public/index.cfm/2022/5/leading-u-s-senators-urge-sec-to-finalize-tough-cybersecurity-disclosure-rules-for-public-companies.

Other members of the United States Congress have also noted their support for the SEC's proposal, as evidenced by comment letters the SEC has received. While enhanced disclosures present potential challenges, some commenters have asserted that the benefits outweigh the concerns because the pervasive impact of cybersecurity threats in business will only increase over time for investors and the public. Those favoring the proposed rule appear to support a need for robust uniformity despite the growing pains and reservations many have, as discussed further below.

But fault lines also exist

Letters received during the comment period point to issues the SEC needs to consider when finalizing the proposal. To no surprise, there are many different views expressed by commenters on the scope and various technical aspects of the proposed rule. The issues articulated generally deal with the prescriptive nature of the proposal. The more significant issues noted by the 139 comment letters[3] are summarized below:

The requirement for immediate disclosure of cyber incidents is too short and may cause unintended consequences to companies and shareholders. The proposal's four-day reporting requirement may be unworkable for two reasons. First, analysis of cyber incidents often requires substantial time. Therefore, the proposed disclosure timing could require companies to make complex materiality determinations in the early stages of a forensics examination while many of the underlying facts are unknown and evolving. The pressure to disclose could result in speculation by preparers, resulting in misleading information and investor confusion.

Second, premature public disclosure without certainty that the threat has been extinguished could compromise ongoing investigations that could lead to the recovery of stolen funds or apprehension of bad actors. The proposal even notes that many states have laws on the books allowing companies to delay public disclosure of a cybersecurity incident if law enforcement determines that such disclosure will interfere with a civil or criminal investigation. There also is fear of unintended consequences. For example, premature disclosure could alert a hostile actor who is still active in the issuer's compromised environment, prompting the actor to leverage alternative tactics or pursue additional exploits to mask intrusions more effectively. It could also provide the attack community

[3] "Comments on the Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure," available at www.sec.gov/comments/s7-09-22/s70922.htm.

access to useful intel with which to expand attacks or carry out additional attacks against issuers reporting unresolved cyber vulnerabilities.

Bottom line, many commenters advanced the view of "delayed disclosure" under certain circumstances, as discussed above. The SEC's consideration of this feedback will be interesting to watch as some may perceive the determination as to when an ongoing investigation is actually concluded as subject to interpretation.

The definition of reportable cyber incidents is too expansive. Many commenters observe that the Commission may be underestimating the sophisticated forensic analysis and subjective judgment required in assessing and managing cyber attacks properly. Following are some considerations raised:

- Defining a cybersecurity incident as "an unauthorized occurrence on or conducted through an issuer's information system" that "jeopardizes" an issuer's "information system" or "information residing therein" is viewed by many commenters as too broad because it may include incidents where no injury or measurable impact has occurred to date. Accordingly, many commenters suggest that the definition of reportable cyber incidents be narrowed, e.g., to those events the issuer has determined to be a cause of a material impact to the company. In asserting that disclosure oriented around attempted attacks would be excessive, commenters did not appear to deny the importance of learnings internally from such attempts.

- Some commenters suggest that the disclosure framework should reflect certain key points, e.g., state data breach statutes, the complexity of assessing materiality of cyber incidents, the need to allow issuers to remediate vulnerabilities before public disclosure, and an exemption for requests from law enforcement or national security agencies to delay disclosure. Notwithstanding that calls by many commenters for the SEC to harmonize its reporting requirements with other federal and state cyber incident reporting protocols is an important theme in the feedback, it is doubtful this will happen any time soon.

- As for aggregating immaterial cybersecurity events for purposes of disclosure, some commenters request clarification as to how the aggregation procedure should be accomplished as well as the relevant period over which the aggregation should be performed. Other commenters recommend that aggregation not be required at all, asserting that the volume and frequency of cyber incidents are such that the

information associated with unrelated events could result in information of little consequence to investors while also posing significant compliance challenges.

- Still other commenters assert that the SEC has not provided a compelling justification for enhancing the incident disclosure rules previously issued in the 2011 Staff Guidance and the 2018 Interpretive Release. Underpinning this assertion is the argument that many registrants already disclose material cybersecurity incidents in accordance with the previous SEC staff guidance and that the proposed rule does not provide any compelling evidence that the existing cybersecurity disclosure guidance is not currently being followed by registrants. To this point, the SEC staff has observed that certain cybersecurity incidents reported in the media were not disclosed in the respective registrant's filings. The reality is it is impossible to determine with certainty the number of material cybersecurity incidents that either are not being disclosed or are not being disclosed in a timely manner.
- Finally, some commenters suggest the SEC align its definition of a cybersecurity incident with the definition used in authoritative frameworks, e.g., the National Institute of Standards and Technology (NIST).

Disclosures of how a company organizes its cybersecurity program may be too granular. The proposal mandates disclosures of a company's cybersecurity policies and procedures and oversight of cybersecurity risk "in such detail as necessary." The specificity of the requirements, as enumerated in the proposal, is viewed by many commenters as too prescriptive, appearing to focus more on the form—versus the substance—of management's review processes. As a result, some perceive the proposal could result in overly detailed filings that have little value to investors. Many point out that disclosure of a company's cybersecurity risk oversight, strategy, policies and procedures could provide intel to malicious actors, spawning significant new threats. There is also the question raised by a few commenters regarding how issuers should consider third-party service providers and the responsibilities of these providers to the companies they serve. In summary, many favor a more principles-based approach to these disclosures.

The board cybersecurity expert disclosure may set a de facto standard that is overly prescriptive and difficult to implement. The comment letters express a number of concerns regarding the commission's proposed rule requiring disclosure of the board's cybersecurity expertise:

- The talent pool is not sufficient to fill the demand for cybersecurity expertise, given the scope of the current proposal. Many commenters point out that there are not enough individuals with both cybersecurity expertise and other relevant experience to make them suitable candidates for corporate board service.

- Between the lines, commenters appear to be pointing out that the rule's implicit narrowing in on cybersecurity expertise does not consider the diverse backgrounds and experiences that contribute to a successful, diverse board. While some may argue that the concept of "fit" constrains the assessment of candidates, commenters expressed concern that boards may be pressured to appoint a technical cybersecurity expert, regardless of whether it is appropriate for their particular governance needs. Thus, there is a fear of unintended consequences as it is unclear how investors might interpret a company's lack of disclosure of a board-level cybersecurity expert, e.g., investors might reach the mistaken conclusion that a company and its board are not concerned with cybersecurity.

- Finally, in the search for qualified individuals to serve on boards, smaller and medium-sized companies may be disproportionately disadvantaged, triggering the need for phasing in this and other aspects of the proposed rule for such companies. (This point is discussed further below.)

The reality is that a one-size-fits-all approach to this requirement is not supported by many commenters. Not all cyber risk landscapes are alike. Many boards are relying—and, as a matter of necessity, may continue to rely—on reporting from in-house cybersecurity teams as well as external consultants as dictated by their companies' respective facts and circumstances. Thus, many commenters suggest the SEC allow for greater flexibility for companies to explain how their boards and management teams coordinate oversight and management of cybersecurity risks.

Many other matters are raised by commenters for the SEC's consideration. Following are a few:

- **The criteria for determining cybersecurity expertise is vague.** Ambiguous criteria may result in boards reaching inconsistent conclusions about cybersecurity expertise, triggering the potential for investor confusion as well as questions as to the ultimate usefulness of complying with the commission's requirements.

- **Naming a cybersecurity expert could result in the named individual becoming a target.** Commenters point out that certain nation states could place named experts under official surveillance. Hackers may try to embarrass the named directors by publishing their personal data or by taking unauthorized control of their personal devices with the objective of discrediting them. The exposure could serve as a disincentive to board service.
- **Companies should be protected from frivolous securities litigation.** Commenters suggest that issuers not be requested to speculate on hypothetical exposures to "danger or risk" or the cumulative impact of previously disclosed cybersecurity incidents. Further, should the SEC opt not to be flexible on the issue of disclosure timing, they suggest the final rule provide a regulatory safe harbor for incidents where companies are requested to postpone disclosure by law enforcement or national security officials.
- **Smaller companies need additional time to comply.** As noted earlier, the SEC's proposed requirements may disproportionately impact smaller issuers with fewer resources. Many commenters suggest a phase-in period giving these companies more time to adjust in preparation for compliance with the final rule.

These and other comments reflect concerns that the SEC will need to weigh carefully as it seeks to accomplish its disclosure objectives. Registrants' disclosures of both material cybersecurity incidents and cybersecurity risk management and governance have improved since the issuance of the 2011 Staff Guidance and the 2018 Interpretive Release. However, the SEC asserts that current reporting may contain insufficient detail and is inconsistent, may not be timely, and can be difficult to locate.

The proposed enhancements are intended to address these deficiencies. The SEC's task is providing sufficient clarity to the preparer community in addressing the concerns raised during the comment period.

In the meantime, what should companies do now and why?

Issuers should expect the commission to issue a final rule later this year. Whether the effective date for larger companies is immediate or applies to years ending after, say, December 15, 2023, remains to be seen. Smaller companies will likely receive more time than larger companies to implement the new disclosure requirements. The SEC may use the accelerated filer definitions to distinguish those companies that are first in line to comply.

In anticipation of the final rules, leaders would be wise to evaluate their company's cybersecurity infrastructure policies, processes and procedures as well as the business continuity, contingency and recovery plans in place. They should consider the expertise they have in place for assessing and managing cybersecurity risk and implementing cybersecurity policies and procedures. Likewise, directors serving public companies should appraise how the board organizes its oversight of cybersecurity risk. Given cyber threats are a moving target, these steps merit consideration on a periodic basis regardless of what the SEC does.

In addition, companies should stay the course in continuing to assess and manage cyber threats. The threat landscape continues to evolve as cyber criminals are using increasingly sophisticated methods to execute their attacks. With an increase in the prevalence of cybersecurity incidents, there is greater risk of the effect of cybersecurity incidents on registrants, not to mention the overall economy. Large-scale cybersecurity attacks can have systemic effects on the economy as a whole, including serious effects on critical infrastructure and national security.

Elevated insider threats are predicted to continue through either mistakes or malicious theft of important data. The substantial changes in the workplace, with the evolving post-COVID, hybrid environments, create new entry points for threat actors. Ransomware attacks targeting organizations' data or critical infrastructure are on the rise. These attacks disrupt or halt operations, posing a dilemma for management to either pay the ransom and hope the attackers keep their word about restoring access and not disclosing data, or not pay the ransom and attempt to restore operations themselves. Enterprise networks on remote access interfaces such as Remote Desktop Protocols are increasingly targeted, as sophisticated adversaries exploit stolen credentials and identities to amplify ransomware attacks and infiltrate cloud environments.

Companies should be mindful that new cyber attack targets continue to emerge. Following are some examples:

- Since the war in Ukraine began, evolving intelligence indicates there is the threat of Russian state-sponsored cyber attacks on companies and critical infrastructure, as the Russian government explores options for potential targets.
- Business IT and cloud service providers are being targeted to exploit trusted relationships and disrupt supply chains.

- Malicious actors are intensifying attacks on critical cloud infrastructure with more sophisticated next-generation approaches.
- Enterprise risk is coalescing around end points combined with cloud workloads, identities and massive sources of data.
- CrowdStrike Intelligence observed an 82% increase in ransomware-related data leaks in 2021 (2,686 attacks as of December 31, 2021, compared to 1,474 in 2020).[4]
- Log4J, a popular library for logging things in Java applications, received more attention than any other vulnerability, as remote actors can inject arbitrary Java code into affected services.
- The Cybersecurity & Infrastructure Security Agency recently noted that threat actors, likely advanced persistent threat actors, are exploiting unpatched VMWare software vulnerabilities.[5]

Companies should continue to monitor the threat landscape and align their cybersecurity infrastructures accordingly.

[4] "New CrowdStrike Report: Ransomware-Related Data Leaks Increased by 82 Percent in 2021," Homeland Security Today, February 15, 2022, available at www.hstoday.us/subject-matter-areas/cybersecurity/new-crowdstrike-report-ransomware-related-data-leaks-increased-by-82-percent-in-2021/.

[5] "Threat Actors Chaining Unpatched VMware Vulnerabilities for Full System Control," Cybersecurity & Infrastructure Security Agency Alert (AA22-138B), June 2, 2022 (revised), available at www.cisa.gov/uscert/ncas/alerts/aa22-138b.

Summary

Investors and other capital markets participants depend on companies' use of secure and reliable information systems and data to conduct their businesses. A significant and increasing amount of the world's economic activities occurs through digital technology and electronic communications. With the ever-evolving threat landscape, cybersecurity continues to attract investor interests and regulatory scrutiny.

Given the feedback from the comments the SEC received, the big-picture question appears to be how to balance the need for disclosure in a manner that positively impacts the public-private partnerships necessary to defend national cybersecurity and critical infrastructure. The SEC's task is finding common ground that avoids risking company security and protects investor interests. In the meantime, public companies should remain vigilant in strengthening their cybersecurity defenses.

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®