SEC Proposes Expanded Cybersecurity Rules

By Thomas J. DeMayo, Principal, Jonathan Zuckerman, Partner and Ioanna Vavasis, Senior Manager

Earlier in the month, the Securities and Exchange Commission (SEC) proposed amendments to its existing rules to enhance and standardize its cybersecurity regulations. The amendments are designed to provide investors with better information about a registrant's cybersecurity risk management, strategy, governance and exposure to cybersecurity incidents. Although current SEC guidance may require disclosure of cybersecurity risks, policies and procedures and material incidents in a registrant's annual report filing, there are no prescriptive requirements as to the disclosure obligations or level of detail.

Major Disclosure Components

Key elements of the proposal include the following:

- Disclosure in a registrant's annual report filing of management's role and expertise in assessing and managing cybersecurity risks including establishment of policies and procedures for identifying and managing cybersecurity risk, as well as information about a registrant's cybersecurity governance.

- In the event a cybersecurity incident were to occur, the registrant would be required to file a Form 8-K within four business days of when the incident is determined to be material (with the term "material" based on the definition of materiality used in SEC security laws).

- Disclosure in subsequent periodic reports (i.e., Form 10-K and 10-Q) of any material changes, additions, or updates to information that was previously disclosed in the Form 8-K in which the initial incident was reported. Also, any previously unreported individually immaterial incidents would need to be disclosed in periodic reports if they become material in the aggregate.

What Registrants Should Consider Doing Now

With any proposed rule, extreme actions should not be taken until the rule reaches a final form; however, the current requirements, as written, align with what is considered current best practice. The SEC increasingly views cybersecurity risks as material considerations that require transparency for investors in registrant reporting. With the heightened political climate over the Russian invasion of Ukraine, it is likely that recent events will serve as a catalyst for the SEC to adopt the proposed rule in its current form as well as consider additional future proposed cybersecurity-related rules.

As a registrant, there is no time better than the present to re-evaluate your cybersecurity risk management practices. A key component of those practices will be to ensure cybersecurity risks are addressed at both governance and management levels. While many larger or well-established registrants will have dedicated security teams and established Chief Information Security Officers, smaller registrants or registrants in development or growth stages often do not have the same level of internal cybersecurity capability that will allow management and those charged with governance to effectively understand and manage the cyber risk. For smaller registrants, external consultants or the adoption of a part-time Virtual Chief Information Security Officer (vCISO) may be a practical and cost-effective alternative to advise management and/or the Board on cybersecurity risks and the effectiveness of the registrant's cybersecurity program.

Registrants may also want to consider having a cybersecurity expert or separate committee to the Board of Directors.

Applicability of Proposed Rules

The proposal applies to all public companies, including foreign private issuers and smaller reporting companies and would provide consistent cybersecurity disclosures for all registrants. If the rules are

finalized as currently proposed, certain provisions will be subject to interpretation and judgment, including the application of the definitions of materiality and cyber incident.

Comment Period

The comment period ends of May 9, 2022. For a complete version of the proposed rule, click here.

How We Can Help

At PKF O'Connor Davies, LLP we have a team of cybersecurity professionals and Virtual Chief Information Security Officers (vCISOs) ready to assist registrants to assess, mature and implement their cybersecurity programs.

Contact Us

If you have any questions about these new proposed rules applicable to SEC-regulated companies – or any other accounting and auditing matters – please contact any of the following or the partner in charge of your client account:

Thomas J. DeMayo, CISSP, CISA, CIPP/US, CRISC, CEH, CHFI, CCFE
Principal, Cybersecurity and Privacy Advisory
tdemayo@pkfod.com

Jonathan Zuckerman, CPA
Partner
jzuckerman@pkfod.com

Ioanna Vavasis, CPA
Senior Manager
ivavasis@pkfod.com