SEC Adopts Amendments on Cybersecurity Disclosure Rules

By Thomas DeMayo, Partner; Rachel DiDio, Partner and Michael Corcione, Partner

On Wednesday, July 26, 2023, the Securities and Exchange Commission (SEC) voted to adopt amendments to its existing rules to enhance and standardize its cybersecurity regulations. The amendments were first proposed in March 2022. The adoption of the amendments further demonstrates the SEC's commitment to provide investors with better information about a registrant's cybersecurity risk management, strategy, governance and exposure to cybersecurity incidents.

Significant Disclosure Components

Key adopted amendments include the following, as noted in the final rule here:

- Registrants will be required, based on the determination of materiality, to disclose on the new Item 1.05 of Form 8-K any cybersecurity incident that will have a material impact on revenues, stock performance, or business operations.
- The report must be filed four business days after a registrant determines that a cybersecurity incident is material and not the date of the actual incident occurrence. Delays will be accepted only upon notification in writing to the SEC that such immediate disclosure, as determined by the United States Attorney General, would pose a substantial risk to national security or public safety.
- Registrants will be required to describe their established cybersecurity program and the associated processes for assessing, identifying and managing material risks from cybersecurity threats, the material effects that may occur from various identified cybersecurity threats or prior incidents that occurred.
- Registrants will need to describe in their annual 10-K, the Board of Directors' oversight of cybersecurity risks and management's role and qualifications of overall cyber risk management.

What Registrants Should Do to Prepare

Consistent with our guidance when the amendments were first proposed, registrants should evaluate or re-evaluate their cybersecurity risk management practices and ensure their program is effectively designed to identify, protect, detect and respond to cyber threats as well as rapidly disclose material cyber incidents. 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 which reports to the Board of Directors.

How We Can Help

At PKF O'Connor Davies we have a team of experts who focus on risk and compliance for SEC registrants, cybersecurity professionals and Virtual Chief Information Security Officers (vCISOs) ready to:

- Assist registrants review or report cybersecurity disclosures.
- Assess, mature, or implement their cybersecurity programs.
- Develop, mature, or test their incident response plans.

A full listing of our services and capabilities can be found here.

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:

Rachel DiDio, CPA
Partner
SEC Regulatory
rdidio@pkfod.com

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

Michael Corcione
Partner
Cybersecurity and Privacy Advisory
mcorcione@pkfod.com