TX Office: (817) 416-6842
NV Office: (702) 565-2727

Kral Ussery
Certified Public Accountants
Advisors - Litigation Support - Internal Audit

March 24, 2022

A Look at the SEC's Proposed Rule to Standardize Disclosures regarding Cybersecurity

A cybersecurity risk management program is prudent for all

By Pete Nassos, CPA, CISSP, CPCU, CITP, CGMA
Principal of Kral Ussery LLC

The U.S. Securities and Exchange Commission (SEC) on March 9, 2022, issued a Proposed Rule and Press Release to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and cybersecurity incident reporting by public companies. There is a 60-day comment period, so if you are passionate about this topic feel free to comment in accordance with instructions in the Proposed Rule. This article summarizes the Proposed Rule, along with comments from the SEC Chairman, Gary Gensler (in favor) and Commissioner Hester Pierce (in dissent). It also explores the evolution and practice of current SEC reporting rules that support the Sarbanes – Oxley Act of 2002 (SOX) and the COSO *Internal Control – Integrated Framework*, as well as business and governance practices towards supporting a robust cybersecurity strategy.

Key Points of Proposed SEC Rules

The SEC has historically released a series of observations and guidance on cybersecurity disclosures for the purpose of improving overall transparency of cybersecurity policies and procedures to strengthen investors' ability to evaluate cybersecurity practices and incident reporting. These efforts enhance the public's ability to determine investment risk, especially since corporate data analytics, IT internal controls, and interconnected network operations between management, customers, and vendors have become increasingly important. Critical data breaches that have been making headlines over the past decade proving that cybersecurity is an emerging risk in causing wide-spread economic damage. Despite significant lessons learned, we often hear of a new major breach or threat action, which in many situations prove that corporate management was not prepared due to insufficient internal controls and cybersecurity hygiene practices. These rules, and growing calls for government mandated governance, echo the evolution and legislation of SOX reporting and governance practices.

Key points of the Proposed Rule were captured from a March 9, 2022, speech by SEC Chairman Gary Gensler (Chair Gensler Speech). Chair Gensler states: *Today's release would enhance issuers' cybersecurity disclosures in two key ways:*

- *First, it would require mandatory, ongoing disclosures on companies' governance, risk management, and strategy with respect to cybersecurity risks. This would allow investors to assess these risks more effectively. For example, under the proposed rules, companies would disclose information such as:*

  - *management's and the board's role and oversight of cybersecurity risks;*
  - *whether companies have cybersecurity policies and procedures; and*
  - *how cybersecurity risks and incidents are likely to impact the company's financials.*
- *Second, it would require mandatory, material cybersecurity incident reporting. This is critical because such material cybersecurity incidents could affect investors' decision-making.*

Specific proposed rules from the SEC's March 9, 2022, release include:

- Material data breach to be publicly reporting within 4 days
- More detailed reporting about the attack, especially about the nature of the data breached or locked up by ransomware
- Improved periodic SEC 8-K filings regarding:
  - Cyber risk management
  - Governance (including board level cyber expertise)
  - Strategy to mitigate risk and provide rapid incident response
- Calls for consistent, comparable, and investor decision useful disclosure standards (like the SOX legislation)
  - Statement of management's role & expertise in assessing and managing cybersecurity risk, as well as implementing cybersecurity policies and procedures (like the annual *Management's Annual Report on Internal Control Over Financial Reporting* requirement)
  - Annual reporting/proxy disclosure on board oversight of cybersecurity risk and expertise (like disclosing if a financial expert is on the Audit Committee, and if not why)

SEC Commissioner Hester Peirce offered a dissenting statement and perspective to the Proposed Rule on March 9, 2022 (Commissioner Peirce Speech). Commissioner Peirce states: *Our role with respect to public companies' activities, cybersecurity or otherwise, is limited. The Commission regulates public companies' disclosures; it does not regulate public companies' activities. Companies register the offer and sale, and classes of securities with the Commission; they themselves are not registered with us, and we do not have the same authority over public companies as we do over investment advisers, broker-dealers, or other registered entities. The proposal, although couched in standard disclosure language, guides companies in substantive, if somewhat subtle, ways.*

- *First, the governance disclosure requirements embody an unprecedented micromanagement by the Commission of the composition and functioning of both the boards of directors and management of public companies. The proposal requires issuers to disclose the name of any board member who has cybersecurity expertise and as much detail as necessary to fully describe the nature of the expertise.*
- *Second, the proposal requires issuers to disclose whether they have a chief information security officer, her relevant expertise, and where she fits in the organizational chart. Third, the proposal requires granular disclosures about the interactions of management and the board of directors on cybersecurity, including the frequency with which the board considers the topic and the frequency with which the relevant experts from the board and management discuss the topic.*
- *Third, the proposal requires granular disclosures about the interactions of management and the board of directors on cybersecurity, including the frequency with which the board considers the topic and the frequency with which the relevant experts from the board and management discuss the topic.*

Commissioner Peirce goes on to use the analogue of the Proposed Rule to the SOX disclosure requirement relating to audit committee financial experts saying that *Congress mandated that foray into corporate governance, which, at least, was directly related to the reliability of the financial statements at the heart of our disclosure system. We are going a step further this time by requiring detailed disclosure about discrete subject matter expertise of directors and employees who are not necessarily executive officers or significant employees, and about the frequency of interactions between the board and management on a specific topic*.

Commissioner Peirce's Speech makes it clear that the integration of cybersecurity expertise into corporate decision-making likely is a prudent business decision; however, issuing such rules by the SEC without the appropriate supporting legislation (like SOX) is not within the SEC's governing mandate. She further notes that the proposed 4-day rule for material breach incident reporting could also have unintended consequences related to interfering with law enforcement activities and potentially causing additional loss.

The analogy and evolution of cybersecurity standards is similar to the development of corporate internal controls and related governance. The Treadway Commission's Committee of Sponsoring Organizations (COSO) developed the original COSO *Internal Control - Integrated Framework* in 1992, and it was revised in 2013. While comprehensive in supporting strong corporate internal control practices, it really did not gain wide-spread application until Congress passed SOX. The SOX legislation provided the foundation for specific governance practices and disclosures, requiring management's adoption of strong internal controls to assure reliability of their financial statements and other disclosures. Misrepresentation of such practices can lead to executives being prosecuted under US Federal law and facing significant fines and possible incarceration.

Complying with the spirit of COSO *Internal Control - Integrated Framework* involves referencing a set of policies and processes (i.e., 'controls'). Similarly, a 'cybersecurity risk management program' (CRMP) is a set of policies, processes, and control activities management puts into place to protect information and systems from security events that could compromise objectives. A CRMP defines the roadmap to detect, respond to, mitigate, and recover from security events in a timely manner.

SOC for Cybersecurity

In a similar approach to improving cybersecurity hygiene and reporting governance, the American Institute of Certified Public Accountants (AICPA) created a cybersecurity risk management reporting framework, "System and Organizational Controls for Cybersecurity" (SOC for Cybersecurity) in 2017. It is oriented towards investors, bankers, management, board members, and other stakeholder to provide an independent opinion from an audit firm and report on the overall cybersecurity practices of the organization. Similar to how an auditor opines on the work of the company's CFO, Controller, and others; the SOC for Cybersecurity report includes an opinion on the work of the company's Chief Information Officer, and Security experts. The SOC for Cybersecurity report details an organization's cybersecurity risk management practices and controls in place to manage a cybersecurity attack.

Few organizations have undertaken a SOC for Cybersecurity examination, likely since they are voluntary as there is no legislation requiring such reports. This may eventually change as cyber-risks continue to increase with no end in sight. Many of the past breaches and resulting losses were caused by lax IT general controls and weak management oversight, as well as not being fully aware of cyber-risks. For instance, the 2021 data breach and pipeline operations shutdown at Colonial Pipeline was a result of a VPN connection that was 'forgotten about' and not monitored or upgraded to current encryption standards. Literally, their backdoor was left open. An

independent, periodic scan of their network would have likely highlighted this deficiency. Identifying and correcting such deficiencies is the objective of the SOC for Cybersecurity process.

The recent hardening of the insurance market to address cybersecurity risk is partially the result of prior insurance coverage being written without clear evidence of appropriate controls. In many cases, the agent or broker provided a cyber-risk checklist to the corporate risk manager, who then had their IT department self-complete the submittal to the insurance company underwriter. Without an independent assessment, which many carriers would demand for coverage of a physical building or inventory, they did not truly understand the risks they were covering. Today, coverage for cyber-risk is more expensive and harder to obtain, with some brokers providing independent scanning and requiring more detailed underwriting criteria, including evidence of appropriate cybersecurity practices. A SOC for Cybersecurity report would be an ideal way to address this.

Conclusion

Adoption of cybersecurity practices such as SOC for Cybersecurity, ISO 27001/ISO 27002, and the National Institute of Science & Technology–Cybersecurity Framework will lead to improved cybersecurity hygiene and comprehensive readiness for incident response. Adapting a sound cybersecurity framework(s) is a crucial element to a successful cybersecurity risk management strategy and an important component to a compressive enterprise risk management (ERM) program. Board members, corporate general counsel, and management need to consider if there has been sufficient implementation and oversight of their CRMP. It's time for all organizations, of any size and industry, to be proactive in combating cyber-risks.

*****

Pete Nassos is a principal of Kral Ussery LLC, a public accounting firm delivering advisory services, litigation support and internal audits. He is a Practice Leader for Insurance & Cybersecurity projects. Contact Pete at PNassos@KralUssery.com.

Kral Ussery LLC serves US public and private companies to protect and grow shareholder value, as well as non-profits and governments with internal controls and in combating fraud. We assist entities in all matters relating to financial reporting, including SEC compliance, internal controls, SOX-404, IT general controls, IPO & SPAC readiness, M&A transactions, US GAAP compliance, and cybersecurity readiness. Visit us at www.KralUssery.com.

This is an article from the Governance Issues™ Newsletter, Volume 2022, Number 1, published on March 24, 2022, by Kral Ussery LLC.