ANDERSON KILL
Cyber Insurance Alert

New SEC Cyber Rules Emphasize Prompt Breach Disclosure Obligations

By Joshua Gold

Key points:

On July 26, the SEC issued its final rule updating disclosure requirements for cyber risk management and cyber incident reporting.

The rule imposes a four-day window for disclosure of material cyber incidents, along with enhanced disclosure of cyber risk management.

Increased liability exposure should prompt companies to ensure that their insurance policies provide adequate protection and do not exclude cyber liabilities.

Last week the U.S. Securities and Exchange Commission announced its long-awaited final rule on cybersecurity and cyber incident reporting obligations. The final SEC rule underscores the importance and obligation of timely disclosure of material cyber incidents. The rule also requires disclosure about corporate risk management and senior management governance of the cyber risk all entities face.

None of the components of the final rule should come as a shock. The SEC's heightened activity over the last several years portended more active enforcement in this arena. Examples include SEC action in the wake of the massive breach of information held by Yahoo, regulatory fines imposed on broker dealers, and, most recently, the SEC's battle with Covington over disclosure of client identities in connection with an alleged data compromise.

Though the final SEC cyber rule is less expansive than the original proposed version, the unmistakable message remains that the SEC intends to step up scrutiny of registrants when it comes to cyber risk management and incident disclosures. This heightened scrutiny places

a spotlight on quality insurance protection: namely, cyber insurance, D&O insurance and crime bonds, no matter the industry of the policyholder.

The SEC Mandate

The Overview to the final rule announces that the SEC is adopting new rules to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incidents by public companies that are subject to the reporting requirements of the Securities Exchange Act of 1934. Specifically, we are adopting amendments to require current disclosure about material cybersecurity incidents. We are

also adopting rules requiring periodic disclosures about a registrant's processes to assess, identify, and manage material cybersecurity risks, management's role in assessing and managing material cybersecurity risks, and the board of directors' oversight of cybersecurity risks.

Short Time Frame To Report Material Cyber Incidents

The SEC provides a short, four-day window to disclose material cyber incidents. Determining whether a cyber incident is "material" may take some time or may become obvious only in hindsight. It is therefore likely that the reporting window will be a source of controversy and contested legal proceedings. The timeline also may vary from time requirements imposed at the state and international level, whether under state notification laws or the EU's GDPR.

Many regulators have indicated informally that any disclosure made more than 30 days from the date of discovery of the incident raises an automatic red flag. Here, the SEC rule requires that:

> An Item 1.05 Form 8-K must be filed within four business days of determining an incident was material. A registrant may delay filing as described below, if the United States Attorney General ("Attorney General") determines immediate disclosure would pose a substantial risk to national security or public safety.

Registrants must amend a prior Item 1.05 Form 8-K to disclose any information called for in Item 1.05(a) that was not determined or was unavailable at the time of the initial Form 8-K filing.

Cyber Risk Governance and Corporate Risk Management

Cyber incident disclosure compliance is not the only risk factor associated with the SEC rule. The SEC has included rules requiring disclosure about corporate cyber risk management and senior management's "governance" of cyber risk. These rules will likely add ammunition to shareholder class action and consumer privacy litigation, as well as regulator scrutiny. As noted in the rule summary:

> Regulation S-K Item 106(b) – Risk management and strategy: Registrants must describe their processes, if any, for the assessment, identification, and management of material risks from cybersecurity threats, and describe whether any risks from cybersecurity threats have materially affected or are reasonably likely to materially affect their business strategy, results of operations, or financial condition.

Regulation S-K Item 106(c) – Governance: Registrants must:

- Describe the board's oversight of risks from cybersecurity threats.
- Describe management's role in assessing and managing material risks from cybersecurity threats.

Manage Cyber Risk Smartly—Whether or Not the Organization Is Within The SEC's Purview

Whether or not an organization is subject to the SEC's regulatory purview, it is prudent for policyholders to follow best practices when it comes to managing cyber risk. These include regular employee training, an informed board, and buy-in from senior management to commit resources and officer-level leadership to develop a robust cybersecurity program. That program should include adequate pre-breach and post-breach planning and protocols, data mapping, sound network

Most important for the board and senior officers is to have a quality D&O insurance program devoid of ANY cyber-related exclusionary language.

architecture to isolate back-up systems to guard against ransomware damage, and prompt dialogue with law enforcement and insurance companies.

Insurance Protection for Cyber Claims and Losses Has Never Been More Essential

With the SEC ratcheting up its scrutiny of public companies (and class action shareholder and privacy suits likely to follow this heightened environment of compliance), policyholders need to ensure that their insurance programs remain capable of protecting the corporation and senior management against these cyber risks. To obtain quality cyber coverage, the input of an expert insurance broker is all but required, given the lack of uniformity in the cyber insurance marketplace. Further, as many cyber insurance policies have exclusions for securities claims, and certain underwriters have increased their attempts to impose cyber exclusionary language on D&O, general liability and other critical commercial insurance policies, it is vital to ensure that the insurance portfolio taken as a whole does not seek to erode coverage for major exposures.

Most important for the board and senior officers is to have a quality D&O insurance program devoid of ANY cyber-related exclusionary language. In recent years, some D&O insurance companies have tinkered with policy language to attempt (sometimes with a sleight of hand) to insert exclusions or limitations in the fine print. This needs to be resisted. If the policyholder is already stuck with such an exclusion in their D&O program (whether in the primary policy or lurking in an excess D&O or Side-A policy), it is wise to get it out of the program ASAP and replace it with a reliable insurance program without gaps or language likely to lead to disputes.

The SEC's "enhanced" cyber rule is no doubt the shape of things to come. Along with developing adequate cybersecurity measures, policyholders will need to ensure that their insurance programs are optimized to cover the "enhanced" liability risks.

JOSHUA GOLD *is a shareholder in Anderson Kill's New York office and is co-chair of the firm's Cyber Insurance Recovery Group. Josh has represented corporate and non-profit policyholders in various industries, with recoveries for his clients well in excess of $1.5 billion. His practice involves matters ranging from data security, international arbitration, directors and officers insurance, business income/property insurance, commercial crime insurance, admiralty, cargo, and marine insurance disputes.*

jgold@andersonkill.com
(212) 278-1886

We are interested in your feedback on topics for future articles and seminars. Please email us.

About Anderson Kill

Anderson Kill practices law in the areas of Insurance Recovery, Commercial Litigation, Environmental Law, Wills, Trusts and Estates, Corporate and Securities, Antitrust, Banking and Lending, Bankruptcy and Restructuring, Real Estate and Construction, Foreign Investment Recovery, Public Law, Government Affairs, Employment and Labor Law, Captive Insurance, Intellectual Property, Corporate Tax, Hospitality, and Health Reform. Recognized nationwide by Chambers USA, and best-known for its work in insurance recovery, the firm represents policyholders only in insurance coverage disputes — with no ties to insurance companies and has no conflicts of interest. Clients include Fortune 1000 companies, small and medium-sized businesses, governmental entities, and nonprofits as well as personal estates. The firm has offices in New York, NY, Newark, NJ, Philadelphia, PA, Washington, D.C., Stamford, CT, Los Angeles, CA, Denver, CO, and Boston, MA.