CHRISTOPHER HETNER
STRATEGIC ADVISOR, SEC EXPERT
HKA

SEC Ramping up Its Cybersecurity Enforcement Actions

This is the second article in a four-part series discussing the involvement of the US Securities and Exchange Commission (SEC) in the ongoing and ever-evolving cybersecurity landscape. This article will discuss the SEC's contemporary cybersecurity priorities, enforcement actions, and suspected future enforcement actions.

To follow up from the SEC's 2018 interpretive guidance on cybersecurity disclosure of public companies, the Commission began ramping up its cybersecurity enforcement actions. As a result of this increased enforcement, a Notice of Proposed Rulemaking, or "NPRM", is expected to be issued by October 21, 2021. After the proposed rule is published, the SEC will specify a time allotment during which the public may review and provide comments to this proposed rule. The SEC will evaluate and consider these public comments as it prepares to publish the final rule. The Office of Information and Regulatory Affairs describes this upcoming rule as intended to "enhance issuer disclosures regarding cybersecurity risk governance." Moreover, the SEC is increasingly focused on taking an active and influential role in the government's wide response to risk mitigation in an increasingly threatening cybersecurity landscape. In the meantime, public companies should begin preparing for what is likely going to be a new SEC rule mandating cybersecurity disclosure.

A Close Look at Cyber-Related Disclosures

Recent enforcement actions from the SEC indicate that the Commission will continue to look closely at cybersecurity-related public disclosures to determine if they are potentially misleading. Such statements often claim either that an entity has strong cybersecurity policies, programs, and systems in place, or to the contrary, that its most important data may have been compromised. Recent SEC enforcement actions reflect scrutiny of entity public statements and even internal disclosures related to cybersecurity vulnerabilities, with a focus on whether the entity was aware of an actual data breach at the time of the statement.

Since the establishment of the SEC's interpretive guidance on aiding public companies in the preparation of their disclosure of cybersecurity risks and incidents, the SEC has stepped up enforcement.

These actions from the SEC also reflect its position that cybersecurity breaches and risks are likely "material" for purposes of disclosure. The SEC's 2018 interpretive guidance defined "materiality" based on consideration of various factors, including the probability of a cybersecurity breach, the magnitude of a past breach, and the importance of compromised data. Therefore, a public company may have to disclose cybersecurity-related affairs in its public filings, thereby fulfilling its requirement to disclose significant cybersecurity risks to its business data, programs, and systems. If, in doing so, a company omits known threats or data vulnerabilities, it could be violating various securities laws.

Since the establishment of the SEC's interpretive guidance on aiding public companies in the preparation of their disclosure of cybersecurity risks and incidents, the SEC has stepped up enforcement. Even more

recently, after the April 2021 Senate confirmation of SEC Chair Gary Gensler, the Commission announced aggressive action to be taken toward public disclosures of cyber risk. This change in initiative, stemming from Chair Gensler's appointment, led to notable cyber-related enforcement action from the SEC.

In June 2021, the SEC announced settled charges against First American Financial Corporation, a financial services entity, for violating disclosure controls and procedures related to a cybersecurity vulnerability that exposed sensitive customer information. First American agreed to pay a penalty of $487,616. Among other things, the SEC found that at the time of the disclosure, the company's information security personnel had been aware of the vulnerability for months.

In August 2021, the SEC announced that Pearson plc, an educational services company, published false statements regarding a cyber breach from 2018. This breach affected several million students across 13,000 school districts and universities. Pearson was also aware that if the company was to experience such an incident, a major confidentiality breach could result. The SEC fined Pearson $1 million and ordered the company to pay the fine within 10 days of the cease-and-desist order litigation.

Proactive Cybersecurity Measures

Reviewing the SEC's 2018 interpretative guidance can provide the C-suite of public companies with sufficient comprehension of the incoming rule. We could anticipate that the Commission will address weaknesses and loopholes in the 2018 guidance, as well as bolster potential deficiencies. While public companies wait for the October 21 deadline, they can take proactive steps to prepare for this new rule.

First, companies should contextualize cyber risk to business, operational, and financial impact by analyzing the materiality of potential exposures. Referring to the SEC's 2018 guidance will provide public companies with some criteria with which to make this determination. Understanding whether a cybersecurity incident constitutes a material event is key. This depends on the nature and magnitude of the incident, along with its potential financial, reputational, or operational ramifications.

> "When cyber risk is a regular agenda item, board directors can bring fresh eyes to the company's risk register and consider ever-evolving circumstances. They can help to promote a disclosure- and compliance-focused culture from the top."

Next, companies should bolster their internal policies and procedures. Developing capable cybersecurity risk management plans, policies, and procedures allows for improved risk mitigation. Specifically, the SEC's 2018 guidance elaborates how these policies should include clear instructions for identifying and elevating information so senior leaders and key stakeholders may adequately disclose any potential cybersecurity incident and risk.

Last, the board of directors has a role in overseeing the disclosure of cybersecurity risks that are material to a company's business. Board members should be encouraged to become more engaged in and focused on the following cyber risk areas:

- *Corporate values*: What risk will we not accept?
- *Strategy*: What are the risks we need to take?

- *Stakeholders*: What risks are stakeholders willing to bear, and to what level?
- *Capacity*: What resources are required to manage those risks?
- *Financial*: Are we adequately understanding the effectiveness of our risk management and harmonizing our spending on risk controls aligned to financial impact?
- *Measurement*: Can we measure cyber risk in economic and business terms and report to senior management and the board in a timely fashion?
- *Management*: Are we effectively managing our risk, with appropriate protocols in place, relative to the company risk profile?

According to Lisa Quateman, a corporate board director and risk committee member with a legal background, this type of analysis should be ongoing so the board and its designated committee(s) are proactive rather than reactive. She says, “When cyber risk is a regular agenda item, board directors can bring fresh eyes to the company’s risk register and consider ever-evolving circumstances. They can help to promote a disclosure- and compliance-focused culture from the top.”

This series of articles is provided courtesy of HKA Global, Inc. (“HKA”) - one of the world’s leading privately owned, independent providers of consulting, expert, and advisory services for the construction, manufacturing, process, and technology industries. HKA’s global portfolio includes prestigious projects on every continent and in varied market sectors.

Christopher Hetner works closely with HKA to provide strategic advice on cybersecurity issues, but he is not an employee of HKA. The information provided in this series of articles represents the opinions only of Mr. Hetner and is intended for general educational purposes only—it does not constitute legal, accounting, insurance, or other professional advice, and it should not be relied upon as the basis for your business decisions.

If you require any further information, please contact Christopher Hetner at christopherhetner@hka.com.