CHRISTOPHER HETNER
STRATEGIC ADVISOR
HKA

The Securities and Exchange Commission's Cybersecurity Stance

This is the first 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 discusses the SEC's public stance on cybersecurity disclosure.

Organizations today operate in an aggressive cyberattack landscape in which threat actors—whether individuals or nation-states—apply constant pressure on them to proactively secure their most valuable assets. As threat actors become more intelligent and technologically advanced, the threat and impact of a potential breach is higher than ever.

Global cybercrime damages are projected to reach $6 trillion in 2021, and nation-state adversaries are increasingly leveraging widely used software suppliers to gain access to networks. The threat of a cyber-driven systemic disruption in the financial sector is so large, in fact, that US Federal Reserve Chair Jerome Powell recently asserted that "the risk that we keep our eyes on the most now is cyber risk."

"As threat actors become more intelligent and technologically advanced, the threat and impact of a potential breach is higher than ever."

As the capabilities of adversaries using cyber to cause harm continue to grow and companies push the boundaries of digital transformation, it is imperative for the C-suite and boards to oversee the development of effective strategies to manage enterprise cyber risk. Indeed, in this environment, many companies see enterprise cyber-resiliency efforts as an opportunity to gain an advantage in today's ultra-competitive economy—rather than just a mere information technology (IT) exercise.

The SEC Vows to be Tougher on Cybersecurity Disclosure

Cybersecurity became a top priority for the SEC in 2011 with the issuance of guidance from their Division of Corporate Finance, requesting and encouraging companies to evaluate their existing disclosure obligations regarding material incidents and cybersecurity risks. This new guidance set the stage for future enforcement, but it became evident that the SEC's strong encouragement didn't gain enough momentum regarding their expectations of both proactive and reactive cyber-risk management.

The SEC's expectation of cyber-risk management became more defined through the unanimous approval of new interpretive guidance. In 2018, the SEC published requirements outlining the disclosure of material incidents and cybersecurity risks for publicly traded companies. The SEC emphasized that cybersecurity risks, and lack of effective risk management, threatens the investors, the capital markets, and the United States.

"Recent enforcement actions confirm that cybersecurity disclosures are a key area of focus for the new SEC leadership."

The current SEC Chair Gary Gensler has pledged to bring a renewed focus to robust enforcement of the federal securities laws. According to a recent blog post by Chair Gensler and Director Gurbir Grewal, the SEC's Division of Enforcement will be more aggressive in several arenas—including public company cybersecurity disclosures. Recent enforcement actions confirm that cybersecurity disclosures are a key area of focus for the new SEC leadership.

With this mounting pressure, companies must continue to advance their cybersecurity risk governance requirements. The current 2018 SEC guidance on public company cybersecurity disclosures encompasses the following four areas pertaining to the management of cyber risk:

Pre-incident disclosure: In the event that a cyber risk is identified, the SEC requires complete transparency from publicly traded companies. The 2018 guidance mandates that these companies provide disclosure on the matter from when the cyber risk is first identified, through the duration of the management process. A company's attack surface continues to expand as it adopts advanced cloud computing, increases its remote workforce, and increasingly relies on a complex supply chain. The SEC requires companies to establish protocols to promptly identify and manage material cyber risks and incidences, in an effort to mitigate risk across company's growing attach surface.

Board oversight: Companies are required to disclose their board's engagement, regarding the internal management of material cyber risks, with the SEC, according to their 2018 interpretive guidance. In an effort to meet these heightened expectations, board members must be transparent and have a contextualized understanding of their business's identified risks.

Incident disclosure: In the event that a material cybersecurity risk or incident is identified, the SEC mandates that companies notify their investors promptly. Having established plans and procedures to identify and determine the materiality

associated with the breach impact on their business and operations, is required under the SEC's 2018 interpretive guidance.

Controls and procedures: Companies are expected to determine the efficacy of their enterprise risk management program as it relates to cyber risk. As cyber risks continue to evolve, ongoing oversight is necessary to identify and manage new risks.

Enforcement Actions Stepped Up

Companies may face enforcement action, resulting in ramifications such as fines and reputational damage, by not observing and following the SEC's guidelines. On June 15, 2021, the SEC announced that it had settled charges against title insurer First American Financial Corporation in connection with a company breach that uncovered and released classified information, due to an internal cybersecurity vulnerability. While First American claimed publicly that it had taken "immediate action" to address the vulnerability, the SEC found that, at the time of the disclosures, the senior executives were not informed of the vulnerability when it was first identified by their information security resources. Furthermore, the vulnerability was not remedied after the initial identification. First American agreed to an order charging the company with failing to maintain adequate cybersecurity disclosure controls and requiring payment of a $487,616 penalty.

"These inadequate internal methodologies would have repercussions for the eight firms, as email accounts were compromised, resulting in thousands of customers sensitive and personal information being exposed."

Then, on August 16, 2021, the SEC announced settled negligence-based fraud and disclosure controls charges against Pearson plc, an educational services company headquartered in London. As stated in the SEC's order, Pearson was notified of a vulnerability on a server used by the company to store sensitive student data, three years prior in 2018. The SEC found that although a patch for the vulnerability was made available to Pearson, the company failed to apply the patch. In March 2019, Pearson learned that the unpatched vulnerability had been exploited by a threat actor who accessed and downloaded 11.5 million rows of student data. Some of the stolen data included students' dates of birth and email addresses.

Additionally, on August 30, 2021, the SEC charged eight firms in three separate actions, citing deficient cybersecurity policies and procedures. These inadequate internal methodologies would have repercussions for the eight firms,

as email accounts were compromised, resulting in thousands of customers sensitive and personal information being exposed. These eight financial institutions were ordered to pay fines totaling $750,000. These charges signified the importance of policy and procedure implementation. Chief of the SEC Enforcement Division's Cyber Unit, Kristina Littman, provided remarks on the charges saying, "it is not enough to write a policy requiring enhanced security measures if those requirements are not implemented or are only partially implemented, especially in the face of known attacks."

Increased Regulation Likely Due to Mounting Pressure

The sheer volume and enormity of recent cyberattacks has caught the attention and raised concerns of investors, regulatory entities, and the US Congress, over the financial industry's cybersecurity and privacy risk management practices. Such threats will likely drive increased enforcement over the compliance of effective and self-managing cybersecurity risk management policies and procedures, as the importance of properly governed cybersecurity programs has never been greater.

In a September 2021 meeting with the US Senate Committee on Banking, Housing, and Urban Affairs, SEC Chair Gensler issued remarks on its cyber agenda: "Staff are developing a proposal for the Commission's consideration on cybersecurity risk governance, which could address issues such as cyber hygiene and incident reporting." Continued enforcement action from the SEC will encourage organizations to develop policies and procedures to manage and minimize their cyber-risk exposure, implement written internal guidelines, and proactively plan and adjust defenses as time progresses and technology improves.

It is important that the cybersecurity C-suite and boardroom communities act now to ensure their digital and cyber risk management efforts are aligned to their business operations and finances (as noted in the current SEC 2018 Cybersecurity Disclosure Guidance). However, many companies may not fully understand—or be fully prepared to meet—these heightened requirements. At a minimum, IT departments can heighten transparency and resultant understanding by translating highly technical jargon into plain language that fully reveals the level of risk companies now face. This plain language can also be used to craft proactive steps that everyone can take—at all organizational levels—to align cyber risk to business, financial, and operational risk exposure and mitigate cyber risk now and in the long term.

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.

HKA