ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

May 6, 2022
Ms. Vanessa Countryman, Secretary
Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549-1090

Re: Cybersecurity Risk Management, Strategy, Governance, and Incidence Disclosure

Dear Secretary Countryman,

The Information Technology and Innovation Foundation (ITIF) is pleased to submit these comments in response to the Securities and Exchange Commission's (SEC) request for public comment concerning the proposed rule on Cybersecurity Risk Management, Strategy, Governance, and Incidence Disclosure.[1] ITIF is a nonprofit, non-partisan public policy think tank based in Washington, D.C., committed to articulating and advancing pro-productivity, pro-innovation, and pro-technology public policy agendas around the world that spur growth, prosperity, and progress.

As SEC correctly identifies, cybersecurity is growing business concern in every industry. Just as the use of information technology (IT) and the collection of data opens businesses up to new opportunities for growth, innovation, and increased efficiency, it also opens them up to new risks. Attackers—including sophisticated state actors, criminal organizations, and insider threats—are constantly developing and employing new techniques that exploit technical or physical security vulnerabilities and human psychology to infiltrate or block access to IT systems and access, steal, alter, or hold data for ransom. Businesses of all sizes and from every sector of the economy can fall victim to cyber attacks, which can cause significant damage in the form of financial loss, intellectual property theft, reputational damage, operational delays, and legal ramifications.

The COVID-19 pandemic exacerbated this problem by shifting even more of Americans' everyday business, communications, and other activities online. In addition, millions of Americans either permanently or temporarily switched to working from home, where their devices and Internet connections may have been less secure than what they would use at their offices. [2]

[1] "Proposed rule: Cybersecurity Risk Management, Strategy, Governance, and Incidence Disclosure," Securities and Exchange Commission, March 9, 2022, https://www.sec.gov/rules/proposed/2022/33-11038.pdf.
[2] Patrick Coate, "Remote Work Before, During, and After the Pandemic," *National Council on Compensation Insurance*, January 25, 2021, https://www.ncci.com/SecureDocuments/QEB/QEB_Q4_2020_RemoteWork.html.

As the need for greater attention to cybersecurity becomes increasingly clear, many investors may wish to consider a firm's cybersecurity practices in order to manage their own financial risk. ITIF supports SEC's efforts to ensure publicly traded companies disclose relevant information on their cybersecurity practices and material cybersecurity incidents, which would enable investors to make more informed decisions, in line with existing SEC disclosure requirements. This type of transparency will not only help investors make more informed decisions, but it should also incentivize companies to adopt cybersecurity best practices.

First, the mandatory, ongoing disclosures of companies' cybersecurity governance, risk management, and strategy listed in proposed Items 106(b) and (c) successfully outline key information that cybersecurity-minded investors are likely to consider. This includes general information about a company's cybersecurity risk assessment and risk management activities, prioritization of cybersecurity in a company's business strategy, and board and management oversight of cybersecurity.

SEC should avoid requiring companies to disclose more detailed information about their cybersecurity governance, risk management, and strategy in order to avoid potentially providing attackers with a "roadmap." However, the amount of detail currently required by the proposed Items strikes an appropriate balance. SEC should also refrain from exempting smaller or emerging companies from these disclosure requirements. Cybersecurity risk affects companies regardless of size. Additionally, smaller or emerging companies are at high risk of going out of business following a data breach or cyber attack. [3] This is a significant risk that investors need to be made aware of.

Second, the mandatory cybersecurity incident disclosure (proposed Item 1.05) is also crucial for investors, given the financial, operational, and reputational impacts cybersecurity incidents may have on targeted businesses. There is an argument for requiring incident disclosure after the incident's impact is quantified or can be reasonably estimated, as SEC acknowledges in its request for comment. However, timely reporting is important for investors to make informed decisions, and determining or even estimating the full extent of an incident's impact can often be a lengthy process. There is room for companies to disclose additional information regarding the extent of an incident's impact, along with other details, once that information becomes available, but the initial disclosure should prioritize timeliness.

There are, however, two details regarding the current cybersecurity incident disclosure requirements in proposed Item 1.05 the SEC should change. First, the current incident disclosure requirements should

[3] Scott Steinberg, Cyberattacks now cost companies $200,000 on average, putting many out of business," *CNBC*, October 13, 2019, https://www.cnbc.com/2019/10/13/cyberattacks-cost-small-companies-200k-putting-many-out-of-business.html.

provide a narrow exception if federal or state law enforcement agencies determine that disclosure would impede an ongoing criminal investigation into the incident. This would benefit investors in cases when a successful law enforcement investigation leads to the recovery of stolen funds or intellectual property. It would also balance the interests of investors against other societal interests, such as prosecuting criminal activity.

Second, SEC should cooperate with the Cybersecurity and Infrastructure Security Agency (CISA) to harmonize proposed cybersecurity incident disclosure requirements with CISA's Incident Reporting System. Companies must already comply with existing data breach notification laws at a state and federal level, and there is an opportunity for SEC to work with CISA to minimize the amount of duplicative work companies must do at least on a federal level.

Overall, SEC's proposed rule strikes a good balance of providing investors with important information regarding cybersecurity risk without providing too much detail that attackers could potentially exploit. The proposed rule would create greater transparency and accountability into cybersecurity risk management and incident response, areas that are of growing concern to many investors given their potential financial, operational, and reputational impact.

Sincerely,

Daniel Castro
Vice President, Information Technology and Innovation Foundation

Ashley Johnson
Senior Policy Analyst, Information Technology and Innovation Foundation