The SEC is inching closer to clarity on cybersecurity requirements

By Jonathan D. Uslaner, Esq., and Jasmine Cooper-Little, Esq., Bernstein Litowitz Berger & Grossmann LLP

APRIL 19, 2023

Cybersecurity is a growing concern for investors and an enforcement priority for the Securities and Exchange Commission ("SEC"). The SEC has recognized that cyber-related threats are "omnipresent" and a serious danger to our capital markets. The investor community and commentators alike recognize that it is imperative that the SEC and courts act swiftly and severely, requiring companies to make robust and immediate disclosures of cybersecurity incidents, as well as implement safeguards to protect against cyberattacks.

The SEC is well positioned to address cybersecurity regulatory concerns. The Commission has followed up on rule-making efforts that began in 2022 and listed three cybersecurity initiatives on its Fall 2022 Unified Agenda of Regulatory and Deregulatory Actions (released in January 2023).

The cybersecurity-focused agenda items include:

(1) Additional rules to address registrant cybersecurity risk and related disclosures;

(2) Rule amendments to better inform investors about a registrant's cybersecurity risk management, strategy, and governance, and to provide timely notification of material cybersecurity incidents; and

(3) Rules to enhance fund and investment adviser disclosures and governance relating to cybersecurity risks.

While certain of these initiatives are in the "Final Rule Stage," it is still unclear whether the SEC will take the actions necessary to improve the cybersecurity-related disclosures and safeguards.

Follow up on last year's cybersecurity projects

In 2022, the SEC took promising steps to protect investors from harmful cyber incidents. To start, on May 3, 2022, the SEC nearly doubled the size of the Enforcement Division's Cyber and Crypto Assets Unit. The full impact of the newly fortified unit is yet to be seen; however, signs are encouraging.

Over the past year, the unit has brought enforcement actions against several SEC-regulated entities for failing to maintain adequate cybersecurity controls and for failing to appropriately disclose cyber-related risks and incidents. The SEC has alleged that these companies violated Regulation S-P, which requires SEC-regulated entities to "adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information."

These SEC enforcement actions have resulted in charges, fines, and settlements. For example, in July 2022, the SEC charged J.P. Morgan Securities LLC, UBS Financial Services Inc., and TradeStation Securities, Inc. for deficiencies in their cybersecurity programs (spanning from January 2017 to October 2019) to prevent customer identity theft. These firms ultimately paid penalties of $1.2 million, $925,000 and $425,000, respectively, to resolve the charges. See press release here: https://bit.ly/3L9UJUg.

The SEC has recognized that cyber-related threats are "omnipresent" and a serious danger to our capital markets.

Then, in September 2022, the SEC ordered Morgan Stanley Smith Barney LLC to pay $35 million for failing to appropriately protect the records and information of 15 million customers, including their personal information and consumer reports. See SEC order here: https://bit.ly/41ucao2.

The SEC's recent cybersecurity enforcement actions are not limited to regulated entities. Individuals are also being held to task for wrongdoing related to cybersecurity breaches. For instance, in August 2022, the SEC brought an action against three individuals for illegally tipping and trading in the securities of Equifax, Inc. in advance of the company's 2017 announcement of a massive cyber intrusion and data breach. Those charged were associated with a public relations firm hired to assist with handling inquiries generated by the announcement of the intrusion and breach.

Two defendants, without admitting or denying the allegations in the SEC's complaint, each consented to the entry of a final judgment, according to the SEC's press release (https://bit.ly/3onTCYk). Those defendants were ordered to disgorge their profit and pay civil penalties, and were permanently enjoined from violating Section 10(b) of the Exchange Act. The third defendant is contesting the charges.

2023 new rule proposals

Keeping up with its momentum, in March 2023, the SEC reopened the comment period for proposed rules and amendments related to cybersecurity risk management and cybersecurity-related disclosure for registered investment advisers, registered investment companies, and business development companies.

The SEC proposed Rule 10, which would, if adopted, require entities to perform critical services to address their cybersecurity risks. Under Rule 10, "market entities" — which includes, among others, broker-dealers and national securities exchanges — must establish, maintain, and enforce written policies and procedures that are reasonably designed to address their cybersecurity risks.

In March 2023, the SEC reopened the comment period for proposed rules and amendments related to cybersecurity risk management and cybersecurity-related disclosure for registered investment advisers, registered investment companies, and business development companies.

The market entities also would need to, at least annually, review and assess the design and effectiveness of their cybersecurity policies and procedures. Further, the market entities would need to give the SEC immediate written electronic notice of significant cybersecurity incidents once the market entities have a reasonable basis to conclude that a significant cybersecurity incident had, indeed, occurred.

If adopted, Rule 10 would require market entities to report cyber risks and incidents to the SEC on a "Form SCIR," part of which would be publicly available. Overall, the rule would help guarantee increased transparency into the innerworkings of market entities and a better assessment of cyber-risks to the U.S. securities markets. The public comment period for the proposed rule is currently open through May 22, 2023.

Public company cybersecurity rules

While the SEC continues to bring enforcement actions and propose cybersecurity rules to govern other regulated entities, shareholders await the SEC's decision on a rule proposed in March 2022 poised to govern public company conduct. The rule would further enhance and standardize disclosure requirements regarding cybersecurity risk management, strategy, governance, and incident reporting.

The SEC's March 2022 proposed rule would specifically require public companies to report material cybersecurity incidents on Form 8-K. The proposed rule would also specifically mandate periodic disclosures regarding a registrant's policies and procedures to identify and manage cybersecurity risks, management's role in implementing cybersecurity policies and procedures, and the board of directors' cybersecurity expertise, if any.

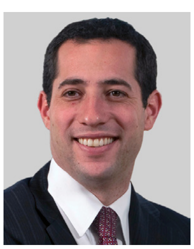
The proposed rule would also require companies to provide updates about previously reported cybersecurity incidents. An SEC rule specific to cybersecurity would provide an additional avenue to punish companies that fail to implement cybersecurity measures and make the proper disclosures.

Conclusion

While the SEC energetically pursues a more cohesive cybersecurity regulatory regime in 2023, only time will tell the implications for the regulated entities and public companies under its jurisdiction. Additional clarity and structure will benefit the SEC and shareholders seeking to put a stop to public companies who fail to make the proper cyber incident disclosures.

Jonathan D. Uslaner is a regular contributing columnist on securities litigation for Reuters Legal News and Westlaw Today.

About the authors



Jonathan D. Uslaner (L) is a partner at **Bernstein Litowitz Berger & Grossmann LLP**, where he prosecutes class and direct actions on behalf of institutional investor clients. He is based in the firm's Los Angeles office and can be reached at jonathanu@blbglaw.com. **Jasmine Cooper-Little** (R) is an associate in the New York office of the firm. Her practice focuses on securities fraud, corporate governance, and shareholder rights litigation on behalf of institutional investor clients. She can be reached at jasmine.cooper-little@blbglaw.com.

This article was first published on Reuters Legal News and Westlaw Today on April 19, 2023.