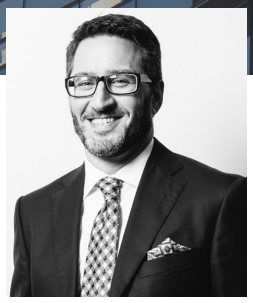
Are Cybersecurity Monitors Part Of The Next Wave For SEC Enforcement?



Randall Lehner
Partner, Kelley Drye
rlehner@kelleydrye.com

Rex Homme
Partner, StoneTurn
rhomme@stoneturn.com

Between the SEC's creation of a specialized cyber unit, its recent release on cybersecurity guidance for disclosures and an emphasis on the need for robust policies and procedures surrounding cybersecurity incidents and reporting, the agency's focus on cybersecurity appears to be at its peak. While the majority of efforts have focused on improving cybersecurity in order to prevent access to non-public information, which could be used for insider trading and related securities laws violations, the senior leadership of the SEC has stated with increasing frequency that enforcement actions against registered entities for inadequate cybersecurity policies, procedures and practices remain a significant consideration for the commission during its investigations. As more enforcement actions are brought for these issues, one of the SEC's increasingly favored remedies—appointed independent consultants and monitors—is likely to be part of any resolution.

Although the SEC has not yet imposed an independent consultant or monitor as part of any cybersecurity-related enforcement actions, it is likely only a matter of time. Accordingly, corporate boards of registered entities and their counsel should consider the implications of a cybersecurity monitor.

> *"Corporate boards, upon learning of a cybersecurity breach or a deficiency in company practices and procedures, should consider proactively hiring an independent monitor to improve cybersecurity practices."*

StoneTurn

Historically, in assessing whether to impose a monitor as part of a settlement, the SEC considers factors such as the nature and pervasiveness of the offense, the length of time of the offense and the remediation and corrective measures the company adopted. Cybersecurity issues may be viewed through a slightly different lens than traditional enforcement actions, since the company is typically the victim in a cyber attack versus a party to misconduct. Nevertheless, the inevitable SEC investigation that follows may uncover that a company was ill-prepared to prevent or detect an attack, which generally indicates that the company did not have an effective compliance program in place. Or worse, the SEC uncovers that the company knowingly ignored red flags or gaps in its program.

Inherent in its mission to "protect investors," the SEC seeks to ensure that companies develop and maintain effective compliance programs. Therefore, it would seem like a logical nexus that the SEC would argue a company's internal controls were not effective in preventing or detecting cybersecurity attacks. Additionally, depending on how, or if, the company discloses a breach to the market, the SEC may also argue that the company's disclosure controls were inadequate, and therefore it did not disclose material information to its investors in a timely or proper manner.

In its evaluation of whether to impose a monitor, the SEC would likely consider the following four questions:

- **Prior to the intrusion (pre-incident), did the company believe it had sufficient and reasonable controls in place and periodically test those controls for effectiveness?**
- **What process did the company use to investigate the issue?**
- **What process did the company use to decide what and when to disclose the intrusion to the market?**
- **Did the company undertake timely and adequate remediation of the issue and how?**

The SEC is likely to place more emphasis on the last two questions. From a disclosure standpoint, Regulation S-K and S-X, governing the filing of non-financial information and the form and content of financial statements included in SEC filings, do not specifically reference cybersecurity. Even if cyber attacks do not quantitatively impact the financial statements, management and the board must assess whether these attacks may be *qualitatively* material and, therefore, need to be disclosed. Management and the board also must assess the risks and whether and when the company should inform its investors when a breach occurs. In essence, can the SEC trust that management and the board are dedicated to maintaining an effective compliance program and to notifying investors of material risks or incidents?

A monitor essentially becomes the eyes and ears of the SEC for a required period of time—often 18 to 36 months—often long after a settlement is reached. Although a monitor creates additional costs for investors, the SEC's imposition of one is meant to ensure a company tries to "do the right thing" to protect investors for the long term—well after the monitoring ends. Corporate boards, upon learning of a cybersecurity breach or a deficiency in company practices and procedures, should consider proactively hiring an independent monitor to improve cybersecurity practices. This approach can yield not only benefits to demonstrate active remediation if the breach or deficiency is disclosed to investors and the SEC, but it also can help insulate the company against accusations that it did not do enough to prevent a future breach or other cybersecurity deficiency.

About the Authors

Randall Lehner is a partner with Kelley, Drye & Warren. He focuses on assisting public and private companies, investment advisers and regulated professionals with government regulatory and enforcement investigations and litigation involving claims of misrepresentation, non-disclosure, conflicts of interest, mismanagement and/or fraud.

Rex Homme is a partner with StoneTurn. He focuses on advising audit committees, boards, senior management and outside counsel with cases involving risk assessments, financial restatements, accounting irregularities, accounting defense, Foreign Corrupt Practices Act ("FCPA") violations, fraud and embezzlement, and financial due diligence.

This article was initially published in
Corporate Board Member in April 2018