MDO | PARTNERS
LAW | COMPLIANCE | ETHICS
Alerts

APRIL 3, 2018

The SEC Releases New Cybersecurity Guidance

The U.S. Securities and Exchange Commission (the "SEC") recently published its 2018 interpretative guidance on cybersecurity matters applicable to U.S. public companies. The guidance focused on three issues:

- Disclosure requirements
- Compliance policies and procedures
- Insider trading

The SEC started to formally address cybersecurity issues in 1999, following the enactment of the Gramm-Leach Bliley Act. However, it wasn't until its 2011 guidance that the SEC directed public companies to use the SEC disclosures as a tool to address cybersecurity issues.

In its 2018 guidance, the SEC addresses the recent increase in cyberattacks and highlights that even companies that have not suffered any attacks should consider the guidance in order to comply with all disclosure requirements. The guidance is an important resource for companies to comply with their already existing duties to their investors, and may lead to the creation of related laws in the future.

Disclosure Requirements

Under the 2018 guidance, the SEC reiterates the obligation set forth in its 2011 guidance for public companies to inform investors about any material cybersecurity risks and incidents in a timely manner, including companies which have not yet suffered an attack but are subject to material cybersecurity risks. The SEC encourages companies to continue using Forms 8-K or 6-K to disclose material information promptly, including material cybersecurity incidents.

The 2018 guidance is the first time that the SEC addresses the materiality of cybersecurity risks and incidents as a factor in determining the duty to disclosure. According to the guidances, the materiality of a cybersecurity issue is determined according to the "likelihood that a reasonable investor would consider the information important in making an investment decision". Factors which determine the materiality of the cybersecurity information are:

- Nature of the incident
- Extent of the cybersecurity issue
- Probability of future incidents
- Potential magnitude, etc.

Moreover, the targeted areas for disclosure of cybersecurity incidents include litigation costs, harm to reputation, intellectual property loss, etc.

Compliance Policies and Procedures

Under the securities laws, public companies are required to maintain effective disclosure controls and procedures. In its 2018 guidance, the SEC clarifies that such requirements extend to cybersecurity incidents and risks. Specifically, the SEC explains that such disclosure controls must focus on ensuring the timely collection of information relating to a company's ability to record, process, summarize, and report information relating to cybersecurity disclosures and related risks.

Insider Trading

The 2018 SEC guidance also addresses the risk of insider trading in public companies regarding information about cybersecurity risks and incidents. The SEC states that such information may be material and thus subject to the insider trading restrictions and prohibitions. The SEC also encouraged companies to explicitly include specific instructions in their code of ethics and insider trading policies to prevent insider trading on cybersecurity information. Further, the SEC directs companies to adopt comprehensive restrictions on insider trading following a cybersecurity incident and during investigations.

The SEC and the Department of Justice are actively enforcing insider trading on cybersecurity. Indeed, last month they charged Jun Ying, a former CIO of Equifax, with insider trading for exercising all of his options right before the company's disclosure of the company's September 2017 data breach. The SEC is seeking disgorgement of profits plus interest, penalties, and injunctive relief. The 2018 guidance comes in light of the risks of insider trading in such cybersecurity incidents, as an issue to be addressed in a company's response plan.

With the additional scrutiny by the SEC and DOJ of disclosure requirements and insider trading relating to cybersecurity, it has become critical for companies to establish or enhance their Cybersecurity Compliance Programs, including conducting a cybersecurity risks assessment, adopting robust procedures and internal controls to protect sensitive information and responding to cyberattacks in a timely manner. In light of the SEC 2018 guidance, MDO Partners encourages companies to enhance their disclosure controls and update their insider trading policies relating to cybersecurity. Our attorneys and advisors have experience advising clients on the cybersecurity matters and effective compliance programs.

If you have questions or comments regarding this Alert, please contact the attorney listed below.

Richard Montes de Oca
Managing Partner
305.704.8452
rmontes@mdopartners.com