Aon Risk Solutions
Financial Services Group

Client Alert: 2018 SEC Cybersecurity Disclosure Guidance – Cyber Risk is D&O Risk

Following a number of noteworthy cybersecurity breaches involving U.S. businesses, on February 21, 2018, the U.S. Securities & Exchange Commission ("SEC") released its Cybersecurity Disclosure Guidance ("Guidance"). The Guidance is intended to provide suggestions for public companies when preparing disclosures about cybersecurity risks and incidents, and communicates the SEC's views on the importance of maintaining comprehensive policies related to cybersecurity. We believe the Guidance aligns an SEC focus area with the emerging trend that "Cyber Risk is D&O Risk."

In concert with the SEC's guidance, SEC Chairman Jay Clayton shared a statement on this Guidance:

In today's environment, cybersecurity is critical to the operations of companies and our markets. Companies increasingly rely on and are exposed to digital technology as they conduct their business operations and engage with their customers, business partners, and other constituencies. This reliance on and exposure to our digitally-connected world presents ongoing risks and threats of cybersecurity incidents for all companies, including public companies regulated by the Commission. Public companies must stay focused on these issues and take all required action to inform investors about material cybersecurity risks and incidents in a timely fashion.

From the Guidance, several recommendations and observations relevant to Directors' and Officers' Liability Insurance emerge:

- *Carefully Determine Materiality Specific to Your Organization* - The SEC disclosure requirements cite "materiality" as the threshold for determining whether any matter, including a cyber incident, must be disclosed to an investor. According to the Guidance, the standard of materiality as determined by the U.S. Supreme Court in TSC Industries v. Northway, 426 U.S. 438, 449 (1976), is that, a fact is material "if there is a substantial likelihood that a reasonable shareholder would consider it important" in making an investment decision or if it "would have been viewed by the reasonable investor as having significantly altered the 'total mix' of information made available to the shareholder." The SEC reminds companies that it must tailor its disclosures to that company's particular cybersecurity risks and incidents, further mentioning that companies should avoid generic cybersecurity disclosures. The SEC also identifies several accommodative considerations with regard to materiality determination, including the recognition that companies are not expected to disclose information that could compromise its cybersecurity defenses, that it may take time for a company to evaluate an incident and determine materiality, and that required cooperation with law enforcement may affect the scope of disclosure.

- *Timely and Comprehensive Disclosure is Critical* - As Chairman Clayton noted, timely reporting is expected. The Guidance specifies that, "Where a company has become aware of a cybersecurity incident or risk that would be material to its investors, we would expect it to make appropriate disclosure timely and sufficiently prior to the offer and sale of securities..." The SEC further affirmatively states that ongoing investigations – both internal and external – do not, on their own provide a reason for companies to avoid timely disclosure of a cybersecurity incident.

We're here to empower results

If you have questions about your specific coverage or want more information, please contact your Aon broker.

www.aon.com

Empower Results®

- *Ensure Board Oversight of Cybersecurity* - The Guidance reminds companies that, "disclosure about the board's involvement in the oversight of the risk management process should provide important information to investors about how a company perceives the role of its board and the relationship between the board and senior management in managing the material risks facing the company." The Guidance further advises that, particularly at those companies where cybersecurity risks are material to a company's business, companies should disclose the nature of the board's involvement with oversight of cybersecurity. These specific comments by the SEC, along with prior litigation targeting the directors and officers of companies with cybersecurity breaches, highlight the importance of board engagement with cybersecurity, as well as the need for public filers to detail to investors the board's engagement to allow investors to make a carefully informed decision with regard to a company's risk management in this area.

- *Insider Trading and Cybersecurity Intersect* - The Guidance reminds companies that issuers, their directors and officers, and other insiders must comply with trading rules regarding material nonpublic information, which can include information related to cybersecurity incidents as well as vulnerabilities. The Guidance reminds issuers that it is illegal to trade securities, "on the basis of material nonpublic information about that security or issuer, in breach of a duty of trust or confidence that is owed directly, indirectly, or derivatively, to the issuer of that security or the shareholders of that issuer, or to any other person who is the source of the material nonpublic information." The Guidance notes that many exchanges require listed companies to adopt policies and a code of conduct that promote compliance with all applicable rules and regulations, including insider trading. The Guidance encourages companies to consider how those codes of conduct address insider trading related to cybersecurity risks, and further prompts issuers to consider prohibiting insider trading while companies are investigating cybersecurity incidents. The Guidance cautions companies to avoid even the appearance of insider trading by implementing stricter disclosure and insider trading protocols.

Conclusion

Public company directors and officers have a duty to understand the ramifications of cybersecurity on their business, and to proactively design risk mitigation procedures and internal disclosure guidelines specific to their company's unique cybersecurity needs. Further, it is believed that the potential for insider trading based upon knowledge of cybersecurity incidents is firmly within the SEC's crosshairs, and possible cause for further corporate governance focus. The SEC's recent Guidance on the cybersecurity topic is believed to signal a growing and continued focus on this matter, and serves as notice that all companies must be prepared.