Derek Kearl

Partner
801.799.5857
Salt Lake City
jdkearl@hollandhart.com

SEC Provides Long-Awaited Guidance on Cybersecurity Disclosures

Insight — 03/05/2018

On February 21, 2018, the U.S. Securities and Exchange Commission ("SEC") released interpretive guidance to assist public companies in the proper disclosure of cybersecurity risks and incidents ("New Guidance") – seven years after the SEC's Division of Corporate Finance first issued guidance on this topic in 2011 ("2011 Guidance"). Significantly, the New Guidance formalizes positions taken by the SEC and its staff since 2011. In that time, companies' exposure to and reliance on networked systems, and the corresponding risks and frequency of cybersecurity incidents have increased exponentially. Public companies, their boards, and senior management must be prepared to appropriately identify and disclose those risks. SEC Chairman Jay Clayton expressed his belief that this New Guidance "will promote clearer and more robust disclosure by companies about cybersecurity risks and incidents, resulting in more complete information being available to investors."

This long-awaited guidance reinforces and expands upon the 2011 Guidance regarding a board of directors' oversight role and a company's disclosure obligations related to cybersecurity incidents and risks. In issuing the New Guidance, the SEC also stressed the importance of two critical areas not covered in the 2011 Guidance: (1) establishing and maintaining comprehensive cybersecurity policies and procedures; and (2) the application of insider trading prohibitions in the cybersecurity context.

Board Risk Management Oversight

Current SEC regulations require a company to disclose the board of directors' involvement in oversight of the risk management process, including providing important information to investors regarding the relationship between the board and senior management in managing material risks facing the company. Where cybersecurity risks are material to a company's business, the New Guidance advises that such disclosures include the nature of the board's role in overseeing the management of those risks. "[D]isclosures regarding a company's cybersecurity risk management program and how the board of directors engages with management on security issues allows investors to assess how a board of directors is discharging its risk oversight responsibility in this increasingly important area."

Disclosure of Cybersecurity Issues

Consistent with the 2011 Guidance, in its New Guidance, the SEC also

reminds companies that existing disclosure requirements pertaining to registration statements, periodic reports, and current reports impose an obligation to disclose cybersecurity risks and incidents in those reports, depending on a company's particular circumstances. Specifically, the New Guidance notes that there are many areas in which disclosure of cybersecurity risks and incidents may be required, including disclosures regarding a company's business and operations, risk factors, management discussion and analysis of financial condition (MD&A), legal proceedings, and financial statements.

In determining their disclosure obligations, companies consider the materiality of cybersecurity risks and incidents. Materiality is always a facts and circumstances determination, and under the New Guidance, whether cybersecurity risks or incidents are material “depends upon their nature, extent, and potential magnitude, particularly as they relate to any compromised information of the business or scope of company operations.” Materiality also depends upon “the range of harm that such incidents could cause,” including harm to the company's reputation, financial performance, and business relationships, as well as possible litigation or regulatory investigations.

When a cybersecurity incident occurs, the SEC recognizes that a company may require time to discern the scope and impact of the incident. However, the New Guidance cautions that an ongoing investigation does not provide a basis for avoiding disclosure of a material cybersecurity incident. Companies also have a duty to update previous disclosures regarding a cybersecurity incident that the company later determines were untrue at the time they were made or otherwise materially inaccurate.

It is also important to note which disclosures companies are not expected to make. The New Guidance is clear that there is no expectation that a company should publicly disclose detailed, specific information about its cybersecurity systems or vulnerabilities that could provide a roadmap for hackers or otherwise compromise its cybersecurity efforts. In sum, under the New Guidance, the SEC expects companies “to provide disclosure that is tailored to their particular cybersecurity risks and incidents,” supplying specific information that will be material and useful to investors. Generic, boilerplate cybersecurity disclosures are discouraged.

Establishing Cybersecurity Policies and Procedures

The New Guidance also encourages companies “to adopt comprehensive policies and procedures related to cybersecurity and to assess their compliance regularly.” Companies should examine their disclosure controls and procedures to ensure that relevant information about cybersecurity risks and incidents is timely reported “up the corporate ladder” to officers and directors who make disclosure decisions and certifications.

The SEC believes that the development of effective controls and procedures “is best achieved when a company's directors, officers, and other persons responsible for developing and overseeing such controls and procedures are informed about cybersecurity risks and incidents that the company has faced or is likely to face.” Specifically, “[c]ontrols and

procedures should enable companies to identify cybersecurity risks and incidents, assess and analyze their impact on a company's business, evaluate the significance associated with such risks and incidents, provide for open communications between technical experts and disclosure advisors, and make timely disclosures regarding such risks and incidents." The New Guidance also notes that, in certifying the effectiveness of such controls and procedures under Sarbanes-Oxley, a company's CEO and CFO should take into account their adequacy in identifying cybersecurity risks.

Insider Trading and Selective Disclosure

Lastly, the New Guidance addresses insider trading and selective disclosure considerations when a cybersecurity incident occurs. It urges companies and their directors, officers, and other corporate insiders to be mindful of laws related to insider trading in connection with information about cybersecurity risks and incidents, including vulnerabilities and breaches. Such information may constitute material, nonpublic information, and corporate insiders may violate anti-fraud provisions of federal securities laws if they trade the company's securities while in possession of that information.

The New Guidance also encourages companies to update insider trading policies to account for, and prevent trading on, material, nonpublic information related to cybersecurity risks and incidents. Specifically, companies should consider whether it may be appropriate to implement restrictions on insider trading while companies are investigating significant cybersecurity incidents and determining facts, ramifications, and materiality of such incidents. They should also consider ways to avoid the appearance of improper trading during the period following an incident and prior to public disclosure of that incident.

The SEC also cautions against making selective disclosure of material, nonpublic information related to cybersecurity risks to investment professionals or other investors before such information is made public, in violation of Regulation FD.

Conclusion

In this ever-evolving landscape of cybersecurity threats, the New Guidance provides critical and timely direction. Given the frequency, magnitude, and costs of cybersecurity incidents, public companies must take action to inform investors about material cybersecurity risks and incidents in a timely fashion. The New Guidance also makes clear that oversight of management of material cybersecurity risks lies not with IT, but with the board and senior management. Development of comprehensive, enterprise-wide policies and procedures to ensure the appropriate evaluation, response, and disclosure of cybersecurity incidents is among the crucial steps companies must take to comply with this guidance.

If you have questions, please contact Derek Kearl at JDKearl@hollandhart.com / (801) 799-5857 or Romaine Marshall at

rcmarshall@hollandhart.com /(801) 799-5922.

Subscribe to get our Insights delivered to your inbox.