Securities Law Alert

Cybersecurity Risk Oversight Obligations of Boards Under Recent SEC Guidance

June 28, 2018

In late February, the Commissioners of the SEC issued guidance emphasizing that Boards of Directors should properly oversee their companies' cybersecurity risks and incidents (the "Guidance"). In addition, the Guidance stressed that public companies should: (i) re-evaluate disclosure controls and procedures as it relates to cybersecurity risks and incidents, (ii) reconsider existing disclosures in this area, and (iii) re-examine their codes of conduct and insider trading policies as they relate to cybersecurity.

I. The Board's Risk Oversight of Cybersecurity

In the recent Guidance, the SEC appears to be encouraging Boards to consider forming a separate Risk Committee over cybersecurity risks to function much like the Audit Committee over financial reporting. If not, some other committee or the full Board will need to be responsible for seeing that management is taking these risks seriously. In addition to regular meetings on this topic to evaluate a company's program to prevent cybersecurity attacks and have in place a team and response plan when an incident occurs, this committee should be meeting in executive session routinely and should consider whether a third-party expert is needed, much like an auditor. This committee could also be responsible for the consideration and review of cybersecurity insurance. Ultimately, the Board or a duly constituted committee must be engaged on this topic, utilize available management resources, understand and assess the adequacy of the measures taken, and demand training and visibility in this area.

II. Disclosure Controls and Procedures

The Guidance stresses the need for expanded disclosure controls and procedures that function effectively to collect cybersecurity-related information and facilitate timely analysis by the disclosure team and the general counsel with a view to timely disclosures in filings with the SEC. One might think this would be well understood by now given the number of material breaches reported in the news, but the SEC felt the need to underscore the role of disclosure controls and procedures in its Guidance. This also means that a company's disclosure controls and procedures should ensure that relevant information regarding cybersecurity risks and incidents is promptly brought to the attention of the designated personnel in order to verify the quarterly certifications related to the effectiveness of such controls and procedures.

In late April 2018, Yahoo! Inc. (now Altaba Inc.) agreed to pay a penalty of $35 million to settle SEC charges that it misled investors by failing to disclose for approximately two years a large data breach in which hackers stole sensitive personal data relating to hundreds of millions of user accounts. The SEC noted that this company's failure to have controls and procedures in place to assess its cyber-disclosure obligations left investors in the dark about this massive data breach. In this case, the SEC faulted management for failing to share information about the incident with the company's auditors or outside counsel as part of the company's assessment of its disclosure obligations in its public filings.

III. Cybersecurity Disclosures

With respect to disclosure obligations generally, the Guidance reinforces and expands upon the guidance issued in 2011 by the SEC's Division of Corporation Finance (the "2011 Staff Guidance"). Companies should consider the materiality of cybersecurity risks and incidents when preparing periodic reports and registration statements for filings with the SEC. In doing so, companies should consider the range of harm that could occur, including harm to its reputation, financial performance, customer and supplier relationships, and litigation or regulatory actions. The Guidance reinforces the 2011 Staff Guidance by stressing the need to consider updating disclosures in five areas: Risk Factors (particularly if there have been prior incidents), known trends and uncertainties in the Management's Discussion and Analysis of Financial Condition and Results of Operations section ("MD&A"), Description of the Business (products, services, relationships with customers and suppliers, or competitive conditions), Legal Proceedings, if any, and Financial Statements to the extent that expenses, revenues, claims, cash flows, assets, liabilities or financing costs are affected. For more guidance on what to take into account in considering the risk of cybersecurity incidents and what to disclose in this regard, see the 2011 Staff Guidance. We can expect the SEC staff to be looking closely at these disclosures in this year's filings.

Should a material breach occur, the SEC can be expected to focus on cases when there is a long gap between a major breach and disclosure as in the recent Yahoo! settlement. While it is possible that companies may determine, in good faith, that their existing risk disclosures cover the incident, those companies should be prepared to explain their process and rationale to the SEC in response to comments related to their periodic filings.

IV. Code of Conduct and Insider Trading Policies

The Guidance reminds companies that information about cybersecurity risks and incidents may be material nonpublic information. The SEC goes on to encourage companies to consider how their codes of conduct and insider trading policies take into account and look to prevent trading on the basis of material nonpublic information related to cybersecurity risks and incidents. The Director of the SEC's Division of Corporation Finance has gone so far as to suggest, if an incident is escalated to the disclosure team to determine materiality, companies may need to consider closing the trading window for those with knowledge of the incident until the company determines whether or not the incident is material. Within weeks after issuing the Guidance, the SEC brought charges against a former Equifax executive, alleging that the executive illegally traded on the basis of information from which he deduced that Equifax had suffered a major data breach before the breach had been publicly disclosed.

What Should Boards Do Now?

- Board Oversight: Re-examine their oversight obligations and how to meet them as it relates to cybersecurity risks and incidents. This may go as far as forming a new Risk Committee given the existing workloads of the other standing committees. Boards should also consider whether a third-party expert should be hired to serve a role similar to auditors with respect to financial information. Companies should be sure to provide a clear delineation of their oversight functions in committee charters and proxy statement risk oversight disclosures.

- Disclosure Controls and Procedures: Evaluate whether existing controls are effective with respect to cybersecurity. The controls and procedures should flag information regarding what could be a serious cyber breach or risk for responsible personnel (possibly including auditors and outside counsel) to facilitate timely materiality assessment to comply with its disclosure obligations. Once an incident is determined to be material, companies should have a plan in place to develop communications to the public.

- Disclosures: Boards should encourage management to review cybersecurity disclosures in the areas identified by the SEC: (i) tailor risk factors and expand

the discussion of cybersecurity issues that create known trends and uncertainties that are material in MD&A; (ii) disclose past attacks, if appropriate, and related costs and consequences of material attacks; (iii) describe aspects of the business and operations impacted by cybersecurity in a significant way; and (iv) explain the company's consideration of the GAAP requirements, including an estimate of reasonably possible losses or range of loss, if reasonably possible.

- Code of Conduct and Insider Trading Policies: Review such policies to ensure that cybersecurity risks and incidents are clearly contemplated. In particular, (i) confirm such matters are included as a type of material nonpublic information and update training to include scenarios involving cybersecurity; (ii) review the ability to impose special blackout periods and ensure that such periods are broad enough in scope and that they cover all personnel who are aware or are reasonably likely to become aware of material nonpublic information; and (iii) review preclearance policies to ensure that the procedure for defining or identifying designated persons who must obtain approval before trading is adequately broad.

For more information on the SEC's cybersecurity guidance, please contact one of the attorneys in our Corporate & Securities Law or Cybersecurity & Data Privacy Practices, including:

Jordan B. Edwards
jedwards@gablelaw.com
Direct dial: 918-595-4865

Stephen W. Lake
slake@gablelaw.com
Direct dial: 918-595-4833

Thomas J. Hutchison
thutchison@gablelaw.com
Direct dial: 918-595-4858

Jeffrey T. Haughey
jhaughey@gablelaw.com
Direct dial: 918-595-4837

Tom C. Vincent II
tvincent@gablelaw.com
918-595-4857

This summary is provided for information purposes based upon our initial review of the Guidance, which could be subject to other interpretation or explanation upon further analysis and review. It does not contain legal advice or create an attorney-client relationship. The information provided should not be taken as an indication of future legal results; and any information furnished should not be acted upon without consulting legal counsel.