KIRKLAND **ALERT**

February 28, 2018

Key Takeaways from the SEC's 2018 Cybersecurity Guidance

Overview

On February 21, 2018, the Securities and Exchange Commission ("SEC") published new guidance regarding public company disclosures about cybersecurity risks and incidents ("2018 Guidance"). As expected, the 2018 Guidance consolidated and built upon the SEC's prior guidance on disclosure obligations relating to cybersecurity, particularly the Division of Corporation Finance's guidance from 2011.

But beyond expanding upon how companies should disclose material information about cybersecurity risks and incidents in compliance with Regulation S-K, the 2018 Guidance also provides several other lessons regarding: (1) the materiality of a cybersecurity risk or incident, (2) the timing of disclosures relating to a cybersecurity incident, (3) disclosures about board oversight, (4) insider trading, (5) cybersecurity policies and procedures, (6) cybersecurity assessments, (7) acquisitions, and (8) regulatory and litigation risk. Taken together, the 2018 Guidance represents an incremental step forward in the evolving cybersecurity and regulatory landscape.

Consistent with the SEC's approach to disclosure, companies will have to develop a tailored approach to materiality determinations and cannot necessarily rely on approaches taken by other companies.

Key Takeaways

Criteria for Determining Materiality. The 2018 Guidance enumerates certain criteria that companies should consider, such as the nature and magnitude of a cybersecurity risk or incident, or the reputational, financial, or operational harm that could result from a cybersecurity risk or incident. Other considerations include potential litigation and/or regulatory actions involving U.S. and non-U.S. authorities. Consistent with the SEC's approach to disclosure, companies will have to develop a tailored approach to materiality determinations and cannot necessarily rely on approaches taken by other companies.

Timing of Disclosures Relating to a Cyber Incident. The 2018 Guidance states that an internal or external investigation into a cybersecurity incident "would not on its own provide a basis for avoiding disclosure of a material cybersecurity incident." This guidance creates tension with some state data breach notification laws that allow companies to delay notifying individuals and/or state regulators if law enforcement determines that notification will impede a civil or criminal investigation. In the coming years, this potential conflict could be resolved through litigation or further guidance.

Board Oversight. The 2018 Guidance states that the Board's role in overseeing cybersecurity risks should be disclosed if "cybersecurity risks are material to a company's business." Such disclosures should address how a Board "engages with management on cybersecurity issues" and "discharge[es] its [cybersecurity] risk oversight responsibility." Given the SEC's position that customers, investors, and the public increasingly rely on security and technology, corporate Board members will have to continue to be vigilant in understanding security and technology and managing cybersecurity risks throughout their organization.

The SEC wrote that companies should have cybersecurity policies and procedures that enable companies to identify and elevate information so that appropriate disclosures regarding cybersecurity risks and incidents can be made.

Insider Trading. The 2018 Guidance encouraged companies to consider how their ethics policies and insider trading policies, as well as "prophylactic measures," can prevent insider trading related to a cybersecurity incident. Companies should review and update their corporate compliance policies relating to insider trading, while also considering the effectiveness of procedural safeguards to minimize insider trading risks, such as implementing a trading blackout in the period following a cybersecurity incident.

Policies and Procedures. The 2018 Guidance encourages companies to develop comprehensive cybersecurity risk management policies and procedures. In particular, the SEC wrote that companies should have cybersecurity policies and procedures that enable companies to identify and elevate information so that appropriate disclosures regarding cybersecurity risks and incidents can be made. Companies should consider reviewing and updating their disclosure controls to confirm that they adequately capture cybersecurity concerns.

Assessments. The 2018 Guidance recommends that companies regularly assess the sufficiency of, and their compliance with, cybersecurity policies and procedures so that information is elevated to appropriate personnel. In order to conduct such assessments, companies should consider a range of options, including manual review of cybersecurity documentation, interviews with key personnel, and interactive readiness tests known as "table top" exercises.

Acquisitions. The 2018 Guidance states that cybersecurity risks arising from acquisitions are among the risks that companies should consider disclosing in the Risk Factors section of periodic filings. This underscores the need for companies contemplating acquisitions to identify and evaluate potential cybersecurity risks through acquisition diligence and post-acquisition monitoring.

Regulatory and Litigation Impact. The 2018 Guidance could also result in increased regulatory enforcement actions and securities litigation. On the regulatory front, the SEC is likely to use the 2018 Guidance as a baseline during OCIE examinations, and given the SEC's frequent public remarks on the topic, SEC cybersecurity enforcement is likely to ramp up. In addition, securities litigation relating to cybersecurity increased substantially in 2017, and the detailed disclosure considerations in the 2018 Guidance might provide another basis for claims regarding material omissions or misrepresentations.

If you have any questions about the matters addressed in this *Kirkland Alert*, please contact the following Kirkland authors or your regular Kirkland contact.

Seth Traxler, P.C.
Kirkland & Ellis LLP
300 North LaSalle
Chicago, IL 60654
www.kirkland.com/straxler
+1 312 862 2241

Asheesh Goel, P.C.
Kirkland & Ellis LLP
300 North LaSalle
Chicago, IL 60654
www.kirkland.com/agoel
+1 312 862 3005

Joshua N. Korff, P.C.
Kirkland & Ellis LLP
601 Lexington Avenue
New York, NY 10022
www.kirkland.com/jkorff
+1 212 446 4943

Gianni Cutri, P.C.
Kirkland & Ellis LLP
300 North LaSalle
Chicago, IL 60654
www.kirkland.com/gcutri
+1 312 862 3372

Erica Williams, P.C.
Kirkland & Ellis LLP
655 Fifteenth Street, N.W.
Washington, D.C. 20005
www.kirkland.com/ewilliams
+1 202 879 5044

Brian P. Kavanaugh
Kirkland & Ellis LLP
300 North LaSalle
Chicago, IL 60654
www.kirkland.com/bkavanaugh
+1 312 862 2015

Sunil Shenoi
Kirkland & Ellis LLP
300 North LaSalle
Chicago, IL 60654
www.kirkland.com/sshenoi
+1 312 862 3028