WHITE & CASE

Client**Alert**

Financial Markets Developments

Capital Markets/Securities
White Collar
November 2011

Cybersecurity Risks and Events Receive SEC Attention—Disclosure Guidance From Corp Fin

The US Securities and Exchange Commission's Division of Corporate Finance ("Corp Fin") recently released guidance regarding the obligation of a publicly traded company or issuer to disclose cybersecurity risks and incidents. Written in response to the increased evidence of concerted, targeted cyber attacks, Corp Fin's issued guidance outlines disclosure considerations and recommends release of information to the market under certain circumstances. The risks associated with cyber penetration could affect financial statements, assessment of controls by management and independent auditors, and certifications required by Sarbanes-Oxley ("SOX").

This new guidance on issuers' disclosure obligations related to cybersecurity threats and incidents introduces additional issues for management to consider and presents new potential risks for management. Existing disclosure rules do not explicitly address cybersecurity. Nevertheless, this new guidance may impose obligations on issuers to disclose material information concerning cybersecurity risks and incidents, in order to make other disclosures, in light of circumstances under which they are made, not misleading or false. As with other operational and financial risks, issuers must review the adequacy of their disclosures related to cybersecurity risks and incidents. This guidance is similar to Corp Fin's interpretive guidance concerning disclosure of climate change matters in so far as it does not create new disclosure standards, but instead emphasizes what Corp Fin wants issuers to consider.

The guidance sets forth specific disclosure considerations and obligations:

Risk Factors

Issuers should disclose risks of cyber events if such incidents are among its significant risks. In determining whether risk factor disclosure is required, issuers are expected to assess all relevant information, including prior cyber incidents and the "severity and frequency of those incidents." Issuers should consider and evaluate the probability and magnitude of a cybersecurity attack or event. As part of this evaluation, issuers should assess the magnitude of these risks, including the costs and consequences of such an event resulting from misappropriation of assets or sensitive information, corruption of data or operational disruption. An assessment should include an evaluation of prior cybersecurity incidents, adequacy of preventative action and known industry risks.

Consistent with Regulation S-K Item 503 (c) requirements for risk factor disclosures generally, cybersecurity risk disclosure must adequately describe the material risks and how each risk affects the issuer, avoiding generic disclosures.

If you have questions or comments regarding this Client Alert, please contact:

G. William Currier
Partner, Washington, DC
+ 1 202 626 3679
wcurrier@whitecase.com

Colin Diamond
Partner, New York
+ 1 212 819 8754
cdiamond@whitecase.com

David Johansen
Partner, New York
+ 1 212 819 8509
djohansen@whitecase.com

George Terwilliger
Partner, Washington, DC
+ 1 202 626 3628
gterwilliger@whitecase.com

White & Case LLP
1155 Avenue of the Americas
New York, NY 10036
United States
+ 1 212 819 8200

White & Case LLP
701 Thirteenth Street, NW
Washington, DC
20005-3807
United States
+ 1 202 626 3600

Depending on the issuer's particular circumstances, appropriate disclosures may include:

- A discussion of aspects of the issuer's business and operations that give rise to material cybersecurity risks and potential costs and consequences
- A description of outsourced functions that present material cybersecurity risks and how the issuer intends to address them
- A description of cyber incidents experienced that are material, either in the aggregate or individually, and costs or consequences of such incidents
- Risks related to potential cyber security events that may remain undetected

To satisfy these requirements, an issuer may have to disclose known or threatened cybersecurity incidents in order to place a discussion of cybersecurity in a meaningful context. Corp Fin's guidance notes that the federal securities laws do not require disclosures that would compromise an issuer's cybersecurity through release of information that could invite attack or otherwise compromise network systems and defenses. At the same time, a specific incident that led, for example, to the destruction of customer data and damage to corporate systems may need to be disclosed in a discussion of specific cybersecurity risks, and known and potential costs and consequences may need to be addressed.

Management's Discussion and Analysis

An issuer should disclose in its MD&A discussion cybersecurity risks or incidents "represent[ing] a material event, trend or uncertainty that is reasonably likely to have a material effect on the issuer's results of operations, liquidity or financial condition." As an example, if material intellectual property is stolen in a cyber attack, the nature and effects of that theft, if material, should be described and the impact on operations should be assessed.

Description of Business

An issuer should disclose cybersecurity incidents that materially "affect an issuer's products, services, relationships with customers or suppliers, or competitive conditions." For example, a product in development adversely affected by a cyber incident should be discussed if the potential impact is material.

Legal Proceedings

An issuer may need to disclose information if material pending legal proceedings involve a cybersecurity event, such as stolen customer information.

Financial Statement Disclosures

Depending on its nature and severity, a cybersecurity incident may impact an issuer's financial statements. For example, such incidents may reveal weaknesses in systems and controls that should be evaluated by the company and assessed by its independent auditors. In addition, an issuer may incur substantial costs in connection with a cybersecurity incident, experiencing losses from claims, including breaches of warranties and contracts, or diminished future cash flows. Although these consequences may not always be apparent when an incident occurs, an issuer should assess and estimate the impact and must explain the risk of a "reasonably possible change in its estimates in the near-term that would be material to the financial statements."

Disclosure Controls and Procedures

Issuers are counseled to consider disclosing cybersecurity incidents that adversely impact its disclosure controls and procedures. For example, if a cybersecurity breach affects the issuer's ability to record financial information properly, its disclosure controls and procedures could be ineffective.

Given the negative impacts and costs of cybersecurity attacks and events, such as remediation costs, costs of increasing cybersecurity, lost revenues, litigation and reputational damage, issuers should reassess their cybersecurity prevention, incident identification and remediation efforts, and current disclosures. Although this guidance does not impose new obligations on companies, it focuses companies on cybersecurity issues and clarifies ambiguity in the disclosure requirements. When preparing financial statements and disclosures, many companies may now need to broaden the scope of review to identify cybersecurity concerns or incidents that may impact the company's performance and trigger disclosure obligations.

Inherent in this guidance is the possibility that if a material event were to occur, and if risk of such an event were foreseen and identified, failure to make appropriate prior cybersecurity disclosures could lead to enforcement review and action by the SEC's Division of Enforcement.

NY1111/CM/A/06591_3