PostScript Picture

# WSGR ALERT

OCTOBER 2011

# SEC STAFF PROVIDES GUIDANCE ON DISCLOSURE OBLIGATIONS RELATING TO CYBERSECURITY RISKS AND CYBER INCIDENTS

The staff of the Securities and Exchange Commission (SEC) recently has begun to publish a new type of informal guidance referred to as "Disclosure Guidance" or a "Staff Observation." Although this guidance represents only the views of the staff and has not been approved by the SEC, it nonetheless provides helpful tips on such matters as reporting and disclosure obligations in specific circumstances based on the staff's experience working with registrants and their counsel.[1]

On October 13, 2011, the staff published its views regarding disclosure obligations related to cybersecurity risks, including risks related to information security.[2] According to the staff, the increasing dependence on digital technologies in the day-to-day operations of nearly every registrant and an increased cybersecurity risk have resulted in greater focus on registrants' disclosure obligations with respect to cybersecurity matters. Although no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents, the staff confirmed its view that a number of disclosure requirements may impose an obligation on registrants to disclose such risks and incidents. As a result, registrants should review, on an ongoing basis, the adequacy of their disclosure relating to cybersecurity risks and cyber incidents, just as they should with any other operational and financial risk.

The staff highlighted the following specific disclosure obligations that may require a discussion of cybersecurity risks and cyber incidents:

- *Risk Factors*. Registrants should disclose the risk of cyber incidents if these issues are among the most significant factors that make an investment in the registrant speculative or risky, with the goal of providing sufficient disclosure to allow investors to appreciate the nature of such risks. As part of evaluating whether risk factor disclosure is appropriate, registrants should examine their cybersecurity risks, ranging from information breaches to systemic attacks, as well as the adequacy of preventative actions taken to reduce such risks. Known or threatened cyber incidents may need to be disclosed to place the discussion of cybersecurity risks in context.

- *Management's Discussion and Analysis of Financial Condition and Results of Operations (MD&A)*. Registrants should address cybersecurity risks and cyber incidents in their MD&A if the costs or other consequences associated with one or more known incidents or the risk of potential incidents represent a material event, trend, or uncertainty that is reasonably likely to have a material effect on the registrant's results of operations, liquidity, or financial condition, or would cause reported financial information not to be necessarily indicative of future operating results or financial condition.

- *Description of Business*. Appropriate disclosure (evaluated on a reportable segment basis) should be made if one or more cyber incidents materially affect a registrant's products, services, relationships with customers or suppliers, or competitive conditions.

- *Legal Proceedings*. Disclosure may be required if a material pending legal proceeding involves a cyber incident.

- *Financial Statement Disclosure*. Cybersecurity risks and cyber incidents may impact a registrant's financial statements both prior to an incident (e.g., costs incurred to prevent such risks and incidents) and during and after an incident (e.g., mitigation of damages, losses incurred in connection with an incident, diminished future cash flows, and estimates developed to account for the financial implications of some or all of the above). For cyber incidents discovered after the balance sheet date but prior to the issuance of financial statements, registrants also should evaluate the need for recognized or nonrecognized subsequent event disclosure.

---

[1] The first in what appears to be an ongoing series of such guidance was issued on September 14, 2011, and dealt with disclosure topics unique to Forms 8-K filed to report reverse mergers and similar transactions. It is available at http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic1.htm.

[2] The full text of the guidance is available at http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

*Continued on page 2...*

## *SEC Staff Provides Guidance . . .*

*Continued from page 1...*

- *Disclosure Controls and Procedures.* Registrants should consider whether a cyber incident has posed (or has the potential to pose) a risk to the registrant's ability to record, process, summarize, and report information required to be disclosed in SEC filings, and, if so, whether as a result there may be any deficiencies in the registrant's disclosure controls and procedures that would render them ineffective.

Securities law disclosures specifically related to information-security concerns have been more prevalent since the adoption of Sarbanes-Oxley (SOX), and particularly Section 404 of SOX. Reviews and implementation of IT-related internal controls have gained importance as potential risks to businesses' financial statements and the enterprises themselves have increased. The severity of incidents already has led some companies to make information security and hacking-related disclosures. The guidance shows the continuing importance of information security as an emerging corporate disclosure issue.

The staff took care to note in the disclosure guidance that it understands the concern of many registrants that detailed disclosures could compromise cybersecurity efforts. It emphasized that the securities laws do not require any disclosure that would itself compromise a registrant's cybersecurity. When evaluating disclosure obligations relating to cybersecurity risks and cyber incidents, registrants should find comfort in the staff's position that its guidance on this topic was prepared to be consistent with the relevant disclosure considerations that arise in connection with any business risk. Stated differently, the staff's view appears to be that the same principles that always have guided registrants in determining what information is required to be disclosed remain relevant with respect to cybersecurity matters.

Nonetheless, the cybersecurity disclosure discussed by the staff is, on the whole, more robust and wide-ranging than the disclosure currently undertaken by most registrants. Going forward, some registrants may need to undertake a more detailed analysis of their cybersecurity risks than they currently perform for purposes of ensuring adequate disclosure. In light of the increased importance of adequate risk disclosure to the staff and others, we believe that the staff's guidance should prompt all registrants to take a careful look at how they manage their disclosure processes surrounding cybersecurity risks and cyber incidents, as the guidance strongly suggests that the staff now views these items as on par with all other business risks.[3]

For more information on these or related matters, or for assistance with evaluating cybersecurity risks or dealing with cyber incidents, please contact your regular Wilson Sonsini Goodrich & Rosati attorney or any member of the firm's corporate and securities or privacy and data security practices.

---

[3] As an initial step, registrants may wish to consider reevaluating whether their information technology function is sufficiently integrated into their ongoing disclosure process, including through adequate participation in disclosure committee meetings.


This WSGR Alert was sent to our clients and interested parties via email on October 18, 2011. To receive future WSGR Alerts and newsletters via email, please contact Marketing at wsgr_resource@wsgr.com and ask to be added to our mailing list.



650 Page Mill Road
Palo Alto, CA 94304-1050
Tel: (650) 493-9300 Fax: (650) 493-6811
email: wsgr_resource@wsgr.com

www.wsgr.com