SIMPSON THACHER MEMORANDUM

Increased Regulatory Focus on Cybersecurity Underscores Need for Public Companies to Review Cybersecurity-Related Disclosures

March 11, 2014

I. RECENT FOCUS ON CYBERSECURITY

As a result of recent highly-publicized data breaches at a number of public companies, lawmakers and regulators have become increasingly focused on the issue of cybersecurity. Renewed attention on cybersecurity is evident, for example, in the various bills pending in Congress that address the issue, such as by seeking to require companies to implement certain data privacy and security standards and to notify customers of breaches within a specified time period. Additionally, in accordance with an executive order issued by President Obama, the National Institute of Standards and Technology recently released its "Framework for Improving Critical Infrastructure Cybersecurity," which provides a set of voluntary "industry standards and best practices to help organizations manage cybersecurity risks."[1] And Securities and Exchange Commission ("SEC") Chairman Mary Jo White testified last month before the U.S. Senate Committee on Banking, Housing, and Urban Affairs that information security is among the 2014 examination priorities of the SEC's National Exam Program.[2]

In addition to increased emphasis on ensuring that companies safeguard personal data and effectively manage cybersecurity threats, recent interest in cybersecurity may mean heightened regulatory scrutiny of public companies' disclosures on cybersecurity risks and threats in their filings with the SEC. Thus, it is crucial that public companies heed the advice of the SEC's Division of Corporation Finance (the "Division") to "review, on an ongoing basis, the adequacy of their disclosure relating to cybersecurity risks and cyber incidents," keeping in mind the Division's 2011 guidance regarding cybersecurity disclosures.[3]

---

[1] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity" (Feb. 12, 2014).

[2] Mary Jo White, Testimony on "Oversight of Financial Stability and Data Security" before the United States Senate Committee on Banking, Housing, and Urban Affairs (Feb. 6, 2014).

[3] Securities and Exchange Commission Division of Corporation Finance, CF Disclosure Guidance: Topic No. 2, Cybersecurity (Oct. 13, 2011).

II. DISCLOSURE GUIDANCE OF THE SEC'S DIVISION OF CORPORATION FINANCE

In 2011, when it issued its guidance, the Division recognized that while there is no disclosure requirement in the federal securities laws explicitly referring to cybersecurity, there are "specific disclosure obligations that may require a discussion of cybersecurity risks and cyber incidents."[4]

1. Risk Factors: If the risk of cyber incidents is among "the most significant factors that make the offering speculative or risky," a registrant must disclose it in its Risk Factors discussion.[5] According to the Division, determining whether risk factor disclosure is required necessitates a registrant's evaluation of its cybersecurity risks, taking into account all relevant information, including:

    - "prior cyber incidents and the severity and frequency of those incidents";
    - "the probability of cyber incidents occurring and the quantitative and qualitative magnitude of those risks"; and
    - "the adequacy of preventative actions taken to reduce cybersecurity risks in the context of the industry" in which the registrant operates, as well as risks to the registrant's cybersecurity system (including threatened attacks).[6]

    As with other risk factors, a registrant's disclosure must be tailored to its specific facts and circumstances – not "a generic 'boilerplate' disclosure" – and must adequately describe each material cybersecurity risk and explain how each risk affects the registrant.[7] This may require disclosure of actual or threatened cyber incidents, as well as the known or potential costs or other consequences stemming from any such incident, to the extent they are material. A registrant need not, however, provide any disclosure that itself would compromise its cybersecurity.

---

[4] *Id*.

[5] Regulation S-K, Item 503(c). As with other risks, a registrant should not "present risks that could apply to any issuer or any offering." *Id*; *see also* CF Disclosure Guidance: Topic No. 2, Cybersecurity.

[6] CF Disclosure Guidance: Topic No. 2, Cybersecurity.

[7] *Id*. According to the Division, "[d]epending on the registrant's particular facts and circumstances, and to the extent material, appropriate disclosures may include: Discussion of aspects of the registrant's business or operations that give rise to material cybersecurity risks and the potential costs and consequences; To the extent the registrant outsources functions that have material cybersecurity risks, description of those functions and how the registrant addresses those risks; Description of cyber incidents experienced by the registrant that are individually, or in the aggregate, material, including a description of the costs and other consequences; Risks related to cyber incidents that may remain undetected for an extended period; and Description of related insurance coverage." *Id*.

2. Management's Discussion and Analysis of Financial Condition and Results of Operations ("MD&A"): Pursuant to the Division's guidance, a registrant should discuss cybersecurity risks or incidents in its 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."[8] In its disclosure, the registrant should include the possible outcomes, if material, of known or potential cyber incidents, such as an increase in cybersecurity protection costs or a reasonable likelihood that the attack will result in reduced revenues.

3. Description of Business: According to the Division, if, upon evaluating the impact of cyber incidents on the registrant's reportable segments, a registrant determines that the incidents "materially affect [the] registrant's products, services, relationships with customers or suppliers, or competitive conditions,"[9] the registrant should include a discussion of the incident and its potential material consequences in its Description of Business.

4. Legal Proceedings: If a registrant or one of its subsidiaries is a party to any material pending legal proceeding involving a cyber incident, information regarding the litigation may need to be disclosed in the registrant's Legal Proceedings disclosure.

5. Financial Statement Disclosures: The Division advised registrants to ensure the proper accounting of costs attendant to cybersecurity and cyber incidents. For example, the Division directed registrants to consider accounting standards relevant to:

    - Capitalization of costs incurred to prevent cybersecurity breaches, if such costs are related to internal-use software;
    - Incentives provided to customers aimed at retaining their business following a cyber incident;
    - Losses from asserted and unasserted claims, "including those related to warranties, breach of contract, product recall and replacement, and indemnification of counterparty losses from their remediation efforts"; and
    - Diminished future cash flows, "requiring consideration of impairment of certain assets."[10]

6. Disclosure Controls and Procedures: In evaluating whether its disclosure controls and procedures are effective, a registrant should consider, among other things, the extent to

[8] *Id.*

[9] *Id.*

[10] *Id.*

which any cyber incidents affect its "ability to record, process, summarize, and report information that is required to be disclosed in Commission filings."[11] If, for example, "it is reasonably possible that information would not be recorded properly due to a cyber incident affecting a registrant's information systems, a registrant may conclude that its disclosure controls and procedures are ineffective."[12]

III. SEC COMMENT LETTERS ON CYBERSECURITY DISCLOSURES

Since the Division issued its guidance two-and-a-half years ago, there has been a significant increase in SEC comment letters to registrants regarding their cybersecurity-related disclosures. In May of 2013, Chairman White indicated that since the publication of the Division's guidance, the SEC's staff "issued comments addressing cybersecurity matters to approximately 50 public companies of varying size and in a wide variety of industries."[13] The number of public companies receiving comments on these issues has further grown since then.

The SEC's comments with regard to companies' disclosures on cybersecurity risks and incidents generally fall into one of four categories:

1. Disclosures Silent About Cybersecurity Risks: Where a company's disclosures do not reference cybersecurity risks, the SEC may request that the registrant provide appropriate risk factor disclosure regarding cybersecurity issues or may ask the registrant what consideration it gave to the Division's guidance to address, among other things, (a) whether the registrant has been subject to any cybersecurity attacks, (b) the adequacy of preventative actions taken to decrease cybersecurity risks, (c) if applicable, the risks resulting from outsourcing of any functions that have material cybersecurity risks, (d) risks related to cyber incidents that may remain undetected for an extended period of time, and (e) whether the registrant has obtained relevant insurance coverage.

2. Disclosures Listing Cybersecurity Risks Among Other Potential Hazards: Where a company's disclosures include cybersecurity risk in a list along with other potential catastrophic events, the SEC may request that in the future, the company provide a separate discussion of risks posed to its operations as a result of the company's dependence on technology or to the company's business, operations, or reputation by cyber attacks. The SEC may also remind the registrant to disclose any actual or attempted cyber attacks it has experienced, in order to put its risk factor disclosure in context.

---

[11] *Id*.

[12] *Id*. In addition to discussing the potential applicability of specific disclosure requirements to cybersecurity risks and incidents, the Division reminded registrants that, as with other matters, "material information regarding cybersecurity risks and cyber incidents is required to be disclosed when necessary in order to make other required disclosures, in light of the circumstances under which they are made, not misleading." *Id*.

[13] Letter from Chairman White to Senator John D. Rockefeller IV (May 1, 2013).

3. General Cybersecurity Disclosures: Where a company's filings provide generally that the company is subject to cybersecurity risks or that computer hacking or other network breaches may materially adversely affect its operations (*e.g.*, "We are subject to cybersecurity risks"), the SEC may ask the registrant what consideration it gave to the Division's guidance (as in number 1, above) or may request that the registrant disclose any security breaches of cyber attacks it has experienced in the past, in order to provide proper context for its risk factor disclosure. In addition, where a company advises the SEC in the comment letter process that it has not experienced any security breaches or cyber attacks that had a material adverse effect on its operations, the SEC often requests that in future filings, the company disclose any cyber incidents that did not result in a material adverse effect on its operations, in order to ensure that investors are aware that the company is experiencing these risks.

4. Disclosures Regarding a Cybersecurity Incident: Where a company discloses a security breach, the SEC may request the disclosure of additional information, often in accordance with the Division's guidance, such as the scope and magnitude of the breach, whether the incident was material, any known or potential costs resulting from the breach, or any preventative measures taken to reduce the risk of future cyber incidents.

IV. CONCLUSION

The SEC continues to actively examine registrants' disclosures and consider disclosure requirements with regard to cybersecurity threats and incidents. In May of 2013, Chairman White noted that she has asked the SEC staff to brief her on public companies' current disclosure practices and their overall compliance with the Division's guidance and requested their recommendations for further action on the issue.[14] More recently, the SEC announced that it will hold a roundtable on March 26, 2014 "to discuss cybersecurity and the issues and challenges it raises for market participants and public companies, and how they are addressing those concerns," including how public companies are disclosing cybersecurity threats and incidents.[15]

In the meantime, registrants should review their cybersecurity-related disclosures and consider their adequacy in light of the Division's guidance. Robust disclosures in compliance with the Division's advice may help prevent (or defeat) a shareholder class action or derivative lawsuit in the event of a data breach followed by a decline in stock price.

---

[14] This request followed an April 9, 2013 letter from Senator John D. Rockefeller IV to Chairman White, opining that despite the Division's guidance, cybersecurity disclosures "are generally still insufficient for investors to discern the true costs and benefits of companies' cybersecurity practices" and urging the SEC to "elevate [the Division's] guidance and issue it at the Commission level as well."

[15] SEC Press Release, "SEC to Hold Cybersecurity Roundtable" (Feb. 14, 2014). The roundtable will be open to the public and webcast live on the SEC's website.

* * *

If you have any questions or would like additional information, please do not hesitate to contact Yafit Cohn at (212) 455-3815 or yafit.cohn@stblaw.com, or any other member of the Firm's Public Company Advisory Practice.

This memorandum is for general information purposes and should not be regarded as legal advice. Please contact your relationship partner if we can be of assistance regarding these important developments. The names and office locations of all of our partners, as well as our recent memoranda, can be obtained from our website, www.simpsonthacher.com.

UNITED STATES

New York
425 Lexington Avenue
New York, NY 10017
+1-212-455-2000

Houston
2 Houston Center
909 Fannin Street
Houston, TX 77010
+1-713-821-5650

Los Angeles
1999 Avenue of the Stars
Los Angeles, CA 90067
+1-310-407-7500

Palo Alto
2475 Hanover Street
Palo Alto, CA 94304
+1-650-251-5000

Washington, D.C.
1155 F Street, N.W.
Washington, D.C. 20004
+1-202-636-5500

EUROPE

London
CityPoint
One Ropemaker Street
London EC2Y 9HU
England
+44-(0)20-7275-6500

ASIA

Beijing
3919 China World Tower
1 Jian Guo Men Wai Avenue
Beijing 100004
China
+86-10-5965-2999

Hong Kong
ICBC Tower
3 Garden Road, Central
Hong Kong
+852-2514-7600

Seoul
West Tower, Mirae Asset Center 1
26 Eulji-ro 5-gil, Jung-gu
Seoul 100-210
Korea
+82-2-6030-3800

Tokyo
Ark Hills Sengokuyama Mori Tower
9-10, Roppongi 1-Chome
Minato-Ku, Tokyo 106-0032
Japan
+81-3-5562-6200

SOUTH AMERICA

São Paulo
Av. Presidente Juscelino Kubitschek, 1455
São Paulo, SP 04543-011
Brazil
+55-11-3546-1000