CARLTON FIELDS

Seeking Clarity on SEC Disclosure Obligations Related to Cybersecurity

July 01, 2015

In response to increasing pressure to update its existing disclosure guidance regarding cybersecurity risks and cyber-incidents, the U.S. Securities and Exchange Commission (the "SEC") is widely expected to overhaul its disclosure rules, including those related to cybersecurity.[1] Until any new rules become final, cybersecurity disclosure obligations will continue to be informed, in part, by the generic SEC "line item" disclosure requirements as well as the general anti-fraud provisions of the federal securities laws, none of which explicitly refer to cybersecurity. Despite the recent surge in reported cybersecurity risks and incidents, the most specific pronouncement on SEC disclosure obligations in this area is a non-binding SEC guidance release from October 13, 2011 ("2011 Guidance").[2] **Increased Cybersecurity Risks Amplify Call for SEC Action** Given the proliferation of incidents and reported risks, new disclosure rules related to cybersecurity are long overdue. Any casual reader of the news over the past several years could readily discern what is now widely recognized, that cyber-incidents have become more frequent, sophisticated, and damaging. Corporate titans across all sectors of industry have been the victims of significant cyber-attacks, including the likes of health benefits company Anthem, entertainment giant Sony Pictures, retailers Target and Home Depot, financial company J.P. Morgan, hospitality company Wyndam Worldwide, and technology company Adobe. Even the United States Federal Government is not immune. Robert S. Mueller, III, former director of the Federal Bureau of Investigation, went as far as to say there are "two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again."[3] From the SEC's point of view, cybersecurity threats are of particular concern because of the widespread and severe impact that cyber-attacks could have on the integrity of the capital markets infrastructure and on companies and investors.[4] In fact, according to SEC Chairwoman White, the SEC's formal jurisdiction over cybersecurity is directly focused on "the integrity of our market systems, customer data protection, and disclosure of material information."[5] In response to the heightened awareness of cybersecurity risks and incidents, the SEC staff has released a panoply of cybersecurity related releases,[6] and held numerous speeches,[7] roundtable discussions,[8]

seminars,[9] and sweep examinations since 2011. It has also identified cybersecurity as an examination priority in both 2014 and 2015.[10] These actions indicate that the SEC's reaction to the growing threat of cybersecurity is consistent with Chairwoman White's insistence that such threats are of "extraordinary and long-term seriousness."[11] Still, there have been efforts by both the legislative and the executive branch to prod the SEC to do more. For example, in April 2013, U.S. Senator John Rockefeller, IV (D-WV) wrote Chairwoman White to request that the SEC issue formal guidance on when companies are required to disclose to investors their cybersecurity risks.[12] While generally complimentary of the positive impact of the staff's guidance on company disclosures, the Senator complained that "the disclosures are still insufficient for investors to discern the true costs and benefits of companies' cybersecurity practices." In December 2014, Congress called upon the SEC to report on its efforts to modernize disclosure requirements, including an update on cybersecurity.[13] The SEC may also be feeling increased pressure "to do its part" based on initiatives from the President calling upon government and industry to ramp up their efforts to address cybersecurity issues.[14] **2011 Guidance on Cybersecurity Disclosure Obligations** The guidance issued on October 13, 2011 by the SEC's Division of Corporation Finance remains the most complete guidance available addressing the application of SEC disclosure rules for cybersecurity risks and cyber-incidents. As acknowledged in the guidance, no existing SEC disclosure requirement explicitly requires disclosure of cybersecurity risks or cyber-incidents. All the same, the guidance goes on to identify the following six areas under Regulation S-K where cybersecurity disclosures may be necessary: **Risk Factors.** Material cybersecurity risks should be disclosed and adequately described as Risk Factors.[15] Part of this analysis includes the probability and potential magnitude of a cyber-incident and the adequacy of the preventative measures taken to reduce such risks relative to the industry in which the registrant operates. The 2011 Guidance further states that appropriate disclosure may include descriptions of cyber-incidents experienced by the registrant that are individually, or in the aggregate, material. **Management's Discussion and Analysis of Financial Condition and Results of Operation (MD&A).** Registrants should disclose cybersecurity risks and cyber-incidents in their MD&A if the consequences associated with any known incidents or the risk of any potential incidents reflect a material event, trend, or uncertainty that is reasonably likely to have a material effect on the registrant.[16] Furthermore, if a cyber-incident prompts a registrant to materially increase its cybersecurity protection expenditures, the 2011 Guidance recommends that the increased expenditures be disclosed even if the original incident itself did not result in any loss. **Description of Business.** Registrants should describe in its "Description of Business" section[17] whether one or more cyber incidents materially affect its products, services, relationships with customers or suppliers, or competitive conditions. **Legal Proceedings.** Registrants should disclose any material pending legal proceeding involving a cyber-incident to which it, or any of its subsidiaries, is a party.[18] **Financial Statement Disclosures.** Cybersecurity risks and incidents that represent substantial costs in prevention or response should be included in Financial Statement Disclosures where the financial impact is material **Disclosure Controls and Procedures.** Where a cybersecurity risk or incident impairs the organization's ability to record or report information that must be disclosed, Disclosure Controls and Procedures that fail to address cybersecurity concerns

may be ineffective and subject to disclosure.[19] The 2011 Guidance, while advising against boiler plate disclosure, does make clear that the SEC staff is mindful of registrants' concerns that overly detailed disclosures could compromise cybersecurity efforts. As such, the 2011 Guidance emphasized that the federal securities laws do not require a registrant to provide, via SEC disclosures, a "roadmap" for those who seek to infiltrate their network security. **SEC Activity after the 2011 Guidance** With more than three years of filing experience under the 2011 Guidance, most registrants are familiar with the requirements stated therein. However, since its issuance, the SEC staff's interpretation of what cybersecurity risks and incidents must be disclosed could arguably be described as evolving. This observation is based on the SEC staff's practice of commenting on registrants' cybersecurity disclosures in periodic reports as well as public statements made by multiple SEC Commissioners. For example, since the 2011 Guidance, it has not been uncommon for the staff to ask a registrant whether it has experienced any cyber-incidents and, if so, to disclose that it has experienced such cyber-incidents, even when the incidents themselves, alone or in the aggregate, are not considered material.[20] In another instance, the SEC staff advised a registrant to consider revising its disclosure stating that a cyber-incident was unlikely. The staff then referred to its considerations set forth in the 2011 Guidance.[21] While these kinds of comments can be frustrating and confusing from a purely analytical perspective, most registrants will simply acquiesce to the staff's request for the additional disclosure and move on. The SEC staff's evolving position on cybersecurity disclosure obligations was also reflected in panel discussions from a roundtable it held on cybersecurity in 2014.[22] During one such panel, Chairwoman White questioned whether there should be a "quicker trigger" than materiality with respect to disclosing cybersecurity risks and incidents.[23] Similarly, during the same 2014 roundtable, Commissioner Stein reportedly questioned whether even non-material cyber-incidents should be disclosed.[24] Such a position is consistent with comments some registrants have received related to disclosure of non-material cybersecurity risks, as described above.[25] The apparent willingness to advocate for, and apply, a standard lower than materiality when determining what cybersecurity related incidents must be disclosed reflects a departure from the 2011 Guidance. In fact, the 2011 Guidance clearly states that cybersecurity disclosures were intended to be "consistent with the relevant disclosure considerations that arise in connection with any business risk." Not surprisingly, the 2011 Guidance is peppered with references to materiality.[26] Shortly after the roundtable, the SEC's Office of Compliance Inspections and Examinations ("OCIE") launched a sweep examination of several registered broker-dealers and investment advisers designed to assess the legal, regulatory, and compliance issues associated with cybersecurity.[27] After sending out questionnaires, the staff then collected and analyzed the information provided by the firms as well as held interviews with key personnel at each firm.[28] An SEC staff summary of the results from the OCIE examinations included the observations that the vast majority of firms reported that they had been the subject of a cyber-incident, including 88% of the brokers and 74% of the investment advisers examined.[29] The summary did not provide any commentary on how the high occurrence rate may influence the staff's policy going forward. Rather, it indicated only that OCIE will "continue to focus on cybersecurity." While the sweep examination was focused on cyber-incidents rather than disclosure,

the results may reinforce the apparent opinion of some on the SEC staff that an aggressive cybersecurity disclosure policy is appropriate. Whether that same aggressive posture is reflected in any new cybersecurity disclosure rules remains to be seen. **Registrants Caught in Disclosure Limbo** Because of the current uncertainty surrounding SEC cybersecurity disclosure obligations, registrants may feel trapped in a catch-22. Disclosing too much may provide a roadmap for those who seek to infiltrate a registrant's network security.[30] Too much disclosure may also attract more regulatory scrutiny, shareholder class actions and derivative lawsuits as regulators and plaintiffs increasingly explore cybersecurity disclosure and related incidents as fertile ground for enforcement actions[31] and for private claims.[32] However, as discussed above, disclosing too little information related to cybersecurity could also draw SEC scrutiny due to insufficient disclosure as well as open the registrant up to litigation claims that it failed to disclose relevant information in the event it suffers a cyber-incident. Statements made at the 2014 roundtable by various SEC Commissioners and staff indicate that the SEC is grappling with these same issues as it considers disclosure requirements.[33] Until new cybersecurity disclosure rules are revealed, registrants should regularly revisit their Risk Factors and other disclosure obligations in light of the 2011 Guidance (and the subsequent shifting interpretations thereof) to determine whether any changes are needed. Furthermore, registrants should be prepared to address any staff comments regarding their cybersecurity disclosures. Registrants should be particularly mindful of this if they have been the recent target of a cyber-incident or have experienced any changes in their cyber-risk profiles since the registrant's last SEC filing.

---

[1] Smeeta Ramarathnam, Chief of Staff to SEC Commissioner Luis Aguilar, Panelist at the RSA Conference, Full Disclosure: What Companies Should Tell Investors about Cyber Incidents (April 23, 2015); see also Cory Bennett, SEC Weighs Cybersecurity Disclosure Rules, The Hill (Jan. 14, 2015), http://thehill.com/policy/cybersecurity/229431-sec-weighs-cybersecurity-disclosure-rules. [2]CF Disclosure Guidance: Topic No. 2, U.S. Sec. & Exch. Comm'n, Div. of Corp. Fin. (Oct. 13, 2011), https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm. [3] Robert S. Mueller, III, Director, Fed. Bureau of Investigation, Speech at the RSA Cyber Security Conference (Mar. 1, 2012), https://www.fbi.gov/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies. [4] Luis A. Aguilar, Commissioner, U.S. Sec. & Exch. Comm'n, Speech at Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus (Jun. 10, 2014), http://www.sec.gov/News/Speech/Detail/Speech/1370542057946. [5] Mary Jo White, Chair, U.S. Sec. & Exch. Comm'n, Opening Statement at SEC Roundtable on Cybersecurity (Mar. 26, 2014), http://www.sec.gov/News/PublicStmt/Detail/PublicStmt/1370541286468. [6] Press Release, U.S. Sec. & Exch. Comm'n, SEC Alerts Investors, Industry on Cybersecurity (Feb. 3, 2015), http://www.sec.gov/news/pressrelease/2015-20.html; Press Release, U.S. Sec. & Exch. Comm'n, SEC Announces Compliance Outreach Program Seminars for Investment Adviser and Investment Company Senior Officers (Apr. 20, 2015), http://www.sec.gov/news/pressrelease/2015-79.html; Press Release, U.S. Sec. & Exch. Comm'n, SEC and FINRA to Hold National Compliance Outreach Program for Broker-Dealers (May 8, 2015), http://www.sec.gov/news/pressrelease/2015-84.html. [7]See, e.g., Aguilar supra note 4; see also White supra note 5. [8]See, e.g., Cybersecurity Roundtable, U.S. Sec. & Exch. Comm'n (Oct. 13, 2011), http://www.sec.gov/spotlight/cybersecurity-roundtable.shtml. [9] See, e.g., Press Release, U.S. Sec. & Exch. Comm'n, SEC Announces Compliance Outreach Program Seminars for Investment Adviser and Investment Company Senior Officers (Apr. 30, 2015), http://www.sec.gov/news/pressrelease/2015-79.html. [10] See, e.g., National Exam Program Examination Priorities for 2015, U.S. Sec. & Exch. Comm'n (2015), http://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2015.pdf; see also National Exam Program Examination Priorities for 2014, U.S. Sec. & Exch. Comm'n (Jan. 9, 2014), http://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2014.pdf. [11] White supra note 5. [12]

Letter from John D. Rockefeller IV, U.S. Senate, to Mary Jo White, Chair, U.S. Sec. & Exch. Comm'n, (Apr. 9, 2013), http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=49ac989b-bd16-4bbd-8d64-8c15ba0e4e51. [13] U.S. House of Representatives Explanatory Statement Submitted by Mr. Rogers of Kentucky, Chairman, U.S. House Committee on Appropriations Regarding the House Amendment to the Senate Amendment on H.R. 83, 113th Congress, 2nd Session Issue: Vol. 160, No. 151 (Dec. 11, 2014); See also Cory Bennett, SEC Weighs Cybersecurity Disclosure Rules, The Hill (Jan. 14, 2015, 6:00 AM), http://thehill.com/policy/cybersecurity/229431-sec-weighs-cybersecurity-disclosure-rules. [14] See Press Release, The White House, SECURING CYBERSPACE - President Obama Announces New Cybersecurity Legislative Proposal and Other Cybersecurity Efforts (Jan. 13, 2015), http://www.whitehouse.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat; See also Eric A. Fischer, Edward C. Liu, John W. Rollins, & Catherine A. Theohary, The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress (Dec. 15, 2014), https://www.fas.org/sgp/crs/misc/R42984.pdf; Exec. Order No. 13636, Improving Critical Infrastructure Cybersecurity, 78 F.R. 11739 (Feb. 19, 2013), http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf. [15] See 17 CFR § 229.503(c) (Item 503(c) of Regulation S-K); 17 CFR § 249.220f ; Form 20-F, Item 3.D. [16] The SEC recently settled securities fraud charges alleging that Bank of America failed to disclose known uncertainties under Regulation S-K. Although the alleged wrongdoing did not involve cybersecurity risks or incidents, it does show the SEC's willingness to pursue reporting companies for their failure to properly assess and disclose trends and unknown risks. See Bank of America Admits Disclosure Failures to Settle SEC Charges, U.S. Sec. & Exch. Comm'n (Aug. 21, 2014), http://www.sec.gov/News/PressRelease/Detail/PressRelease/1370542719632. [17] See 17 CFR § 229.101 (Item 101 of Regulation S-K); Form 20-F, Item 4.B. [18] See 17 CFR § 229.103 (Item 103 of Regulation S-K). [19] See 17 CFR § 229.307 (Item 307 of Regulation S-K); Form 20-F, Item 15(a). [20] See Letter from Suzanne Hayes, Assistant Dir., U.S. Sec. & Exch. Comm'n, to James J. Malerba, Exec. Vice President, Corporate Controller & Chief Accounting Officer, State Street Corp. (Apr. 9, 2012), available at http://www.sec.gov; See also SEC Comment Letters- Including Industry Insights: Constructing Clear Disclosures, Deloitte & Touche, (7th ed. 2013). [21] See Letter from Maryse Mills-Apenteng, Special Counsel, U.S. Sec. & Exch. Comm'n, to Dana Gallovicova, Chief Enforcement Officer, Zlato Inc. (June 11, 2013), available at http://www.sec.gov. [22] Cybersecurity Roundtable, supra note 8. [23] Cybersecurity Roundtable Transcript, U.S. Sec. & Exch. Comm'n (Mar. 26, 2014) at 102, http://www.sec.gov/spotlight/cybersecurity-roundtable/cybersecurity-roundtable-transcript.txt. [24] Id. at 108, (stating "[i]f the materiality standard isn't working in this particular situation in the way it might… what should we be talking about? Should it be principles based, or should there be a floor, and should that vary from industry to industry?"). [25] See Letter from Suzanne Hayes, Assistant Dir., SEC, to James J. Malerba, Exec. Vice President, Corporate Controller & Chief Accounting Officer, State Street Corp. (Apr. 9, 2012), available at http://www.sec.gov; See also Deloitte & Touche, SEC Comment Letters- Including Industry Insights: Constructing Clear Disclosures 67 (7th ed. 2013). [26] See CF Disclosure Guidance, supra note 2. [27] See Cybersecurity Examination Sweep Summary, Office of Compliance Inspections and Examinations, Sec. & Exch. Comm'n, Volume IV, Issue 4 (February 3, 2015), http://www.sec.gov/ocie/announcement/Cybersecurity+Risk+Alert++%2526+Appendix+-+4.15.14.pdf. [28] Id. [29] Id. [30] See CF Disclosure Guidance, supra note 2. [31] See, e.g., Press Releases, supra note 14. [32] Cybersecurity Roundtable Transcript, supra note 23 at 86, (with one commenter observing that "if [a] breach isn't otherwise going to become public, if you suffered a breach, you know that if the breach were to become public, you are now going to be a target of a lot of class action plaintiffs, of consumer protection regulators, who will not look at you as the victim of the breach…but will look at you as almost the perpetrator of the breach."). [33] Cybersecurity Roundtable Transcript, supra note 23 at 13, 98 (Commissioner Aguilar stated that "[t]here is no doubt the SEC must play a role in this area. What is less clear is what that role should be." Additionally, Keith Higgins, Director of Division of Corporation Finance stated "[i]f you take boilerplate [disclosure] on the one hand and on the far side you take a look at the specific road map of the company's vulnerabilities and what the consequences of those vulnerabilities could be, where do you find the balance?...Is there somewhere in the middle that will be helpful to investors while at the same time not harmful to companies.").

Authored By

Edmund J. Zaharewicz

Related Practices

Cybersecurity and Privacy
Technology

Related Industries

Technology