June 2014

Recent Developments Concerning Cybersecurity Disclosure for Public Companies

Cyber incidents have become more common — and more severe — in recent years. Like other federal agencies, the Securities and Exchange Commission (Commission) has recently been analyzing the applicability of its existing regulations relating to cybersecurity risks. The Commission's efforts are focused on maintaining the integrity of market systems, protecting customer data and the disclosure of material information. We provide an overview of recent developments in public company cybersecurity disclosure of particular interest to public companies.

Commissioner Aguilar Speech

In a speech on June 10, 2014, Commissioner Luis Aguilar made remarks on cybersecurity issues during a conference hosted by the New York Stock Exchange. Commissioner Aguilar noted the increasing cost and frequency of cyber attacks on public companies. He also expressed concern as to the severe impact that cyber attacks could have on the integrity of the capital markets and on public companies and investors. The commissioner advocated for boards of directors' having an expanded role in preparing for cybersecurity risks as well as in coordinating responses when breaches occur. He also encouraged companies "to go beyond the impact on the company and to also consider the impact on others." He continued, "It is possible that a cyber attack may not have a direct material adverse impact on the company itself, but that a loss of customers' personal and financial data could have devastating effects on the lives of the company's customers and many Americans." Although Commissioner Aguilar was careful to note that he does not speak for the full Commission, his speech demonstrates that cybersecurity issues continue to concern officials at the highest levels of the agency.

Disclosure Principles

The Commission's Division of Corporation Finance (Division) made its first significant foray into formalizing guidance on public company cybersecurity disclosure in October 2011 with *Disclosure Guidance: Topic No. 2 — Cybersecurity*.[1] There, the Division reiterated that the federal security laws are designed to elicit disclosure of timely, comprehensive and accurate information about risks and events that a reasonable investor would consider important to an investment decision. Thus, although the Commission's existing disclosure requirements do not explicitly refer to cybersecurity risks and cyber incidents, general principles of materiality may nonetheless require a public company to discuss these issues. The Division noted that existing disclosure requirements under Regulation S-K, such as risk factors, MD&A, description of business, legal proceedings and financial statement disclosure, could be implicated by cyber risks and cyber incidents. The guidance was careful to note that companies are not required to make disclosures that could provide a "roadmap" for those who seek to infiltrate a company's network in the future. To the extent cyber incidents pose a risk for a registrant, disclosure controls and procedures may also be implicated. These topics received additional attention at a roundtable on

[1] The complete guidance is available at http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

cybersecurity the Commission hosted on March 26, 2014.[2] And on April 15, 2014, the Commission's Office of Compliance Inspections and Examinations issued a risk alert in which it announced its plans to conduct targeted examinations of more than 50 registered broker-dealers and registered investment advisers with respect to cybersecurity readiness.[3]

In a speech on May 1, 2014, Shelley Parratt, a deputy director of the Division, observed that cybersecurity remains an important focus for the Division as new incidents of hacking emerge. Although the full text of her speech was not made publicly available, media accounts indicate Parratt amplified Disclosure Guidance Topic No. 2 and highlighted the following themes for public companies in crafting cybersecurity disclosures for investors:

- how information submitted to the Commission would be updated as threats evolve and risks change;
- how the company would respond in the event of a material breach;
- whether there are aspects of the company's operations that give rise to material cybersecurity risks;
- the potential consequences and costs associated with cyber incidents;
- whether the company has outsourced functions that expose it to cybersecurity risks; and
- whether the company has experienced a material cybersecurity incident, and, if so, whether its disclosure is current with respect to that incident.

Nevertheless, Parratt reiterated that companies need not make disclosures that would essentially serve as a roadmap of a public company's vulnerabilities.

Staff in the Division has been active in recent years in commenting on public company periodic reports regarding cybersecurity issues. Drawn from publicly available comment letters to registrants, examples of these staff comments read as follows:

- You indicate that you have been subject to ongoing cyber attacks, but that those attacks have not had a material impact upon your operations. We also note that you recently reported unusual activity on your website and news stories indicate that the Company, like other financial institutions, has been subject to cyber attacks and breaches. In order for investors to better understand the extent to which the risk of cyber attacks may impact your business, they must be able to understand the fact that you have experienced attacks. Please revise your disclosure in future filings, starting with your next 10-Q, to disclose that you have experienced attacks to place the risk of cybersecurity breaches in context for your investors.
- It appears that you may have experienced one or more security breaches or cyber attacks that did not result in a material adverse effect on your operations. If true, beginning with your next periodic filing, please simply state this fact so investors are aware that you are currently experiencing these cyber risks.

[2] Various discussion materials, including a transcript of the proceedings, are available at http://www.sec.gov/spotlight/cybersecurity-roundtable.shtml.

[3] The alert is available at http://www.sec.gov/ocie/announcement/Cybersecurity+Risk+Alert++%2526+Appendix+-+4.15.14.pdf.

- We note that it is reported that companies in your industry have been the target of cyber attacks. In your next Form 10-Q, please provide a separate discussion of the risks posed to your operations from your dependence upon technology or to your business, operations or reputation by cyber attacks. In addition, in order to provide the proper context for your risk factor disclosure, and as your letter of response suggests, please confirm that you will disclose that you have experienced cyber attacks.

- We note that you acknowledge that you have been subject, and will likely continue to be subject, to attempts to breach the security of your networks and IT infrastructure through cyber attack, malware, computer viruses and other means of unauthorized access. It does not appear that you have previously disclosed to your investors that this risk is one that you are currently subject to and actively working to prevent. Beginning with your next Form 10-Q, please confirm that you will disclose that you have been subject, and will likely continue to be subject, to attempts to breach the security of your networks and IT infrastructure through cyber attack, malware, computer viruses and other means of unauthorized access.

- We note that you added cyber attacks to the list of potential catastrophic events in this risk factor. In future filings, beginning with your next Form 10-Q, please provide a separate discussion of the risks posed to your operations from your dependence upon technology or to your business, operations or reputation by cyber attacks. In addition, please tell us whether you have experienced cyber attacks in the past. If so, please also disclose that you have experienced such cyber attacks in order to provide the proper context for your risk factor disclosure. Please refer to the Division of Corporation Finance's Disclosure Guidance Topic No. 2 for additional information.

- We note your disclosure that the Company's computer network was the target of a cyber attack that you believe was sponsored by a foreign government, designed to interfere with your journalism and undermine your reporting. We also note your disclosure that you have implemented controls and taken other preventative actions to further strengthen your systems against future attacks. If the amount of the increased expenditures in cybersecurity protection measures was or is expected to be material to your financial statements, please revise your discussion in MD&A to discuss these increased expenditures. Also, if material, please revise the notes to your financial statements to disclose how you are accounting for these expenditures, including the capitalization of any costs related to internal use software.

- We note you disclose that you and your service providers collect and retain significant volumes of certain types of personally identifiable and other information pertaining to your customers, stockholders and employees and that a significant actual or potential theft, loss, fraudulent use or misuse of customer, stockholder, employee or your data by cybercrime or otherwise could adversely impact your reputation and could result in significant costs, fines, litigation or regulatory action against you. We note the disclosure in your latest Form 10-Q referencing prior data breach incidents. Beginning with your next Form 10-Q, please state that you have experienced data breach incidents in the past in order to provide the proper context for your risk factor disclosure. Please refer to the Division of Corporation Finance's Disclosure Guidance Topic No. 2 for additional information.

Shareholder Litigation

Private litigants have also been focusing on public company cybersecurity disclosure. In shareholder litigation arising out of Target's highly publicized 2013 data breach, the plaintiffs have alleged that the company's officers and directors engaged in a pattern of wrongdoing involving breaches of fiduciary duty, gross mismanagement, waste of corporate assets and abuse of control. Specifically, the plaintiffs alleged that officers and directors breached duties of loyalty and good faith by allowing the company to release a series of false and misleading statements to the public describing the data breach, by failing to oversee the company's business and operations, and by failing to monitor practices that resulted in the data breach. The plaintiffs' complaint also alleged that officers and directors made the decision to conceal the

full scope of the breach so as not to impair holiday sales, with the cumulative effect of these actions' being a further erosion of customer confidence and damage to the company' reputation. Shareholder suits against public companies that are making similar allegations are becoming increasingly common in the aftermath of cyber attacks.

Takeaways

Despite calls from some members of Congress and other groups for further Commission guidance on the topic of cybersecurity disclosure, it is not likely the Commission will take any formal action in the near term. Instead, existing law and recent Commission pronouncements should continue to guide public companies in satisfying their disclosure obligations. At a more fundamental level, public companies should address the growing cybersecurity risk head-on. Examples of proactive action for public companies include:

- developing an appropriate enterprise-wide governance structure for addressing cybersecurity;
- identifying and assessing sensitive data;
- developing effective information security policies and procedures;
- calibrating disclosure controls and procedures to encompass cybersecurity disclosure, when material;
- assessing technical, physical and administrative protections on a continuing basis;
- managing employee and vendor cybersecurity risks;
- training personnel to identify risks and manage them appropriately;
- preparing a cyber incident response plan tailored to the unique needs of a public company, including (among other things) protocols for managing investor relations, press releases, communications with regulators/law enforcement and public disclosures in the event of a cyber incident;
- keeping the board of directors and appropriate board committees apprised of compliance efforts and enterprise risks; and
- practicing the cyber incident response plan on a regular basis.

Contacts

Scott H. Kimpel
skimpel@hunton.com

Lisa J. Sotto
lsotto@hunton.com

Paul M. Tiao
ptiao@hunton.com

Aaron P. Simpson
asimpson@hunton.com