The CYBERSECURITY LAW REPORT

www.cslawreport.com Volume 2, Number 11 May 25, 2016

SEC

Key Considerations for Public Companies for Mitigating and Disclosing Cybersecurity Risks

By Richard A. Blunk (Thermopylae Ventures, LLC) and Apprameya Iyengar (Morrison Cohen LLP)

The SEC has continued to emphasize cybersecurity preparedness – making clear it will (i) push public companies to assess and mitigate cybersecurity risks on an ongoing basis and (ii) scrutinize companies' cybersecurity-related disclosures under other disclosure requirements. While SEC Commissioner Mary Jo White recognized that cybersecurity is the most significant risk facing the financial system, the SEC has yet to promulgate any specific requirements forcing public companies to disclose their cybersecurity risks and incidents.

In response, public companies are agonizing over how to proactively mitigate cyberattacks, how much information to include in their cybersecurity disclosures, and when such disclosures should be made.

See also "*Meeting Expectations for SEC Disclosures of Cybersecurity Risks and Incidents*": *Part One* (Aug. 12, 2015); *Part Two* (Aug. 26, 2015).

Questions to Ask and Factors to Consider

Public companies should be constantly examining at least the following areas when making disclosures, tailoring the considerations to the specific cyber risks facing the company.

1) Are the Program Assessments Sufficient?

Directors and officers, as a matter of their duty of care to the company, are obligated to regularly review and assess the adequacy of the company's cybersecurity risks and controls along with other matters affecting the business operations of the company.

As a best practice, the New York Stock Exchange (NYSE) has recommended that a company's cybersecurity risks and controls be overseen by a chief information security officer (CISO) that is organizationally positioned with a strong and independent voice (e.g., reporting directly to the chief executive officer and/or the board of directors) to effectively oversee matters relating to the company's informational security. If a public company chooses to appoint a CISO, then directors and officers should carefully examine whether the CISO has the appropriate staff and resources to implement an effective infrastructure to assess, detect and mitigate cyber vulnerabilities across the enterprise on a regular basis.

At a minimum, a public company's ongoing cyber risk assessments should evaluate:

- *Most Valued and Sensitive Data*
  - Has the company considered where its most valued and sensitive data (e.g., business process data, employee data) is located and who has access to that data?
  - How is access to the company's most valued and sensitive data audited, controlled and monitored?
- *Security Adequacy*
  - What are the biggest vulnerabilities in the company's IT networks (e.g., cloud, email, mobile, Wi-Fi)?
  - What security measures are in place at the perimeter of the company's IT networks to prevent an unauthorized intrusion of the company's systems?
  - How effective are the company's existing IT security protocols (e.g., perimeter and network security) and should more stringent security measures be implemented?
- *Likely Threats.* Is the company aware that savvy cyber criminals may bypass a company's perimeter network security systems through company

employees or third-party contractors accessing compromised websites, third-party applications, "zero day exploits" and malware from the company's networks?

- *Cyber Breach Preparedness*
  - Has the company created and implemented an incident response plan in the case of an actual incident?
  - How often is the company's incident response plan tested and who conducts the testing? Companies should consider engaging independent third parties to review the company's cyber incident response plan to help mitigate the risks posed by current and foreseeable threats.
  - Does the company rectify the material deficiencies identified in such tests? Testing your company's incident response plan may provide valuable insight to exactly how the company would respond in the wake of a cyber attack and understanding gaps in the company's incident response plan.
- *Third-Party IT Services Vendors*
  - What procedures are in place to vet the IT security procedures of the company's third-party vendors providing IT-related services?
  - Does the company know where and how its data will be stored?
  - If the service provider suffers a data breach, what are the vendor's incident notification procedures and how quickly will the provider be able to restore the security of their service?
  - Following a vendor's notification of a breach, what are the company's procedures to respond to its vendor's data breach?
- *Costs of a Breach.* Depending on the company's business operations and specific type of data compromised in a cyber incident, what are the likely costs to comply with applicable breach notification obligations imposed at the state level?
- *Public Relations.* Separate from the company's disclosure obligations of cyber incidents, has the company engaged a public relations firm to help the company craft the public messaging of a cyber incident in the most favorable manner?
- *Insurance*
  - Is the company's cybersecurity insurance coverage adequate in light of the cybersecurity risks the company is exposed to? See "*Don't Overlook Commercial General Liability Insurance to Defend a Data Breach*" (Apr. 27, 2016).
  - Should the company expand the scope of its current cybersecurity insurance coverage and/or should it increase the level of coverage provided by the company's insurer?

See "*How In-House Counsel, Management and the Board Can Collaborate to Manage Cyber Risks and Liability*": *Part One* (Jan. 20, 2016); *Part Two* (Feb. 3, 2016).

2) Are Disclosures Included Under T heir Appropriate Topics?

Existing SEC guidance indicates that cybersecurity risks and incidents should be disclosed in a company's Form 10-K, Form 10-Q, or Form 8-K filing(s), where appropriate, and companies should consider the following topics when making their cyber disclosures:

- *Risk Factors*
  - Companies should consider the Risk Factors section as the primary area to make its cybersecurity disclosures, especially if the inherent nature of a company's business operations could expose the company to the types of cyber risks a reasonable investor would consider to be material when investing in the company.
  - When crafting the appropriate disclosure, companies should consider the magnitude of prior attacks (if any), the likelihood of future attacks and the economic and non-economic effects on the company's business operations.
- *Management's Discussion and Analysis of Financial Condition and Results of Operations (MD&A).* If a cyber risk or incident poses an uncertain trend that materially affects a company's business operations

or its financial condition, the company should consider addressing such cybersecurity risks and/or incidents in its MD&A section.

- *Description of Business*. If a cybersecurity incident has materially affected the company's business operations in the past, companies should also consider making the appropriate cyber disclosure in the Description of Business section of the company's Form 10-K or Form 10-Q filing.
- *Legal Proceedings.* If, as a result of a cyber attack, the company was involved in any significant litigation, it should disclose the facts about the litigation in this section.
- *Financial Statements.* If the company anticipates substantial expenses associated with cyber readiness or for taking corrective action following a cyber attack, then such expenses should be specified in the company's financial statements.
- *Form 8-K, Item 8.01, "Other Events"*
  - Companies may also voluntarily disclose certain cybersecurity incidents that it believes are important to investors through a Form 8-K filing.
  - Notably, as Form 8-Ks apply to specific material corporate events, Form 8-K cyber disclosures should generally be considered if an actual cyberattack occurs.

3) Has the Company Looked at the Whole Picture?

The SEC's interpretive guidance has advised publicly traded companies to disclose cybersecurity risks that a reasonable investor would consider material in making an investment in the company. However, the adequacy of company's cybersecurity risk disclosures may differ based on the nature of the company's business activities. In crafting risk disclosures that are accurate and complete, but do not jeopardize the company's IT security, a public company should carefully consider:

- *Prior SEC Disclosures*
  - What cybersecurity risk disclosures has the company previously made?
  - Coupled with the company's other disclosures, the company is required to update its cybersecurity risk disclosures, so that the company's cybersecurity risk disclosures are accurate and complete in light of prior disclosures made by the company.
- *Disclosures of Peer Companies*
  - What cybersecurity risk disclosures have peer companies made?
  - Do the company's cybersecurity risk disclosures significantly differ from its peer companies in terms of issues raised and the level of detail provided?
- *Understanding the Effects of Cyber Incidents*
  - If the company is in the immediate wake of a breach, has it fully investigated the incident and understood its ramifications? Generally, a company should avoid immediately making public statements or disclosures of actual or alleged cyber incidents until it has collected and understood all of the relevant information regarding a cyber incident in order to ensure that any related disclosures are accurate and not misleading.
  - Once the cyberattack has been verified, companies should consider disclosing the cyberattack in a Form 8-K, Item 8.01, "Other Events."

4) Upsides and Downsides to Voluntary Disclosure

Public companies should carefully consider the specific upsides and downsides to voluntarily disclosing cybersecurity incidents through a Form 8-K filing in each instance. Potential upsides for voluntarily disclosing cybersecurity incidents on a Form 8-K filing may include:

- *Reducing Litigation Exposure*
  - Companies could potentially limit their exposure to securities class action claims that material risks relating to its business operations were not adequately disclosed as of the date of the company's Form 8-K filing.
  - A voluntary disclosure may counter insider-trading allegations (if the suspected trading activity occurred after the Form 8-K filing).

- *Limiting Regulation Fair Disclosure (Regulation FD) Issues*
  - As Regulation FD prohibits companies from making selective disclosures to the general public, a company should investigate whether it made any public statements regarding any breaches it has suffered. Once a company has disclosed a cyber incident to a third party, the company should assume that such a disclosure is likely to be made public, and lean towards making the appropriate disclosure through a From 8-K filing.
  - Depending on the type of data that is compromised (e.g., personally identifiable information), companies should consider whether other laws or contractual obligations compel the company to disclose the incident or if such an incident is likely to be heavily publicized. If the company is under an obligation to disclose a cyber incident or if it is likely that the incident will become well-known to the general public, the company should consider disclosing the cyber incident through a Form 8-K filing as well.
- *Controlling the Public Message of the Cybersecurity Incident.* A voluntary disclosure on a Form 8-K filing can help the company provide details of the incident in the light most favorable to the company, ahead of third parties who may not frame it as positively (e.g., news media or publicity-seeking hacktivists).

On the other hand, the potential upsides of making a voluntary disclosure should also be weighed against the potential downsides, including:

- *Harm to Business Reputation and Stock Price*
  - If the company suffers a cybersecurity incident that is not material and unlikely to be publicized, the disclosure of such an event could unnecessarily expose the company to negative attention.
  - Coupled with harm to the company's business reputation, the company's stock price may drop due to lack of investor confidence regarding the company's cybersecurity controls and procedures.
- *Increased Exposure to Litigation.* In some instances, a voluntary disclosure may increase the company's exposure to litigation from its shareholders arguing that prior to the company's Form 8-K filing the company's cybersecurity risks were not adequately disclosed and/or materially misleading.

- *Additional Cyberattacks on the Company's IT Systems*
  - Companies should be aware that voluntarily publicizing a cybersecurity incident may inadvertently invite additional cyber criminals to attack their IT systems. It is advisable for companies to investigate the incident and neutralize the effects of such an incident before publicizing vulnerabilities in its IT networks.
  - Companies should be mindful of not including superfluous information when disclosing the technical details of a cyber attack to avoid providing a road map for future cyber attacks on the company's IT systems.

In light of the alarming rate that public companies are suffering from cyber incidents and the widespread belief that such breaches may continue to increase in both frequency and severity, public companies should be prepared to be heavily scrutinized by the SEC, despite the lack of specific SEC cybersecurity disclosure requirements. Accordingly, public companies should, on an ongoing basis, prioritize how they manage their cybersecurity risks and carefully consider the adequacy and sufficiency of their cybersecurity disclosures.

www.cslawreport.com Volume 2, Number 11 May 25, 2016

Richard A. Blunk is the managing director and general counsel of Thermopylae Ventures, LLC, a Dallas-based alternative investment group with interests in, among others, alternative litigation finance, cybersecurity and database management and intellectual property monetization as well as investments in, and transactional insurance for, internet addresses.

Apprameya Iyengar is attorney at Morrison Cohen LLP. His practice is primarily focused on the array of commercial technology needs confronting organizations ranging from small and mid-cap emerging companies to Fortune 500 companies, across a broad spectrum of industries. His experience includes drafting and negotiating various types of in-bound and out-bound technology licensing and outsourcing transactions, and counseling clients on the information security issues that often arise in such transactions.

