MINTZ

Cybersecurity Disclosure: A Panel Discussion with the SEC's Division of Corporation Finance

April 09, 2013 | Blog | By Adam Veness, **Cynthia J. Larose**

VIEWPOINT TOPICS

- Privacy & Cybersecurity

RELATED PRACTICES

RELATED INDUSTRIES

Last week in Washington, D.C., this author had the opportunity to sit in on a panel discussion by the SEC's Division of Corporation Finance ("CorpFin") discussing, among other things, recent developments in cybersecurity disclosure in public company filings. The panel included CorpFin's Acting Director Lona Nallengara, Deputy Director of Disclosure Operations Shelley Parratt and others from CorpFin.

One question asked of the panel was whether companies are actually listening to the **SEC Guidance issued in late 2011**. The panel acknowledged that it has seen improvement in public company disclosure related to cybersecurity (consistent with what **we previously reported here**), and that the 2011 guidance is still very relevant. The panel disclosed that the SEC has issued cybersecurity comments to approximately 50 public companies since issuing its guidance. Specifically, the panel outlined the three major types of cybersecurity comments that the SEC has issued:

1) **Disclose Specific Cybersecurity Breaches**: Although public companies are beginning to include greater disclosure related to how data breaches *could* occur, the SEC has issued comments requesting that companies disclose whether data breaches *have actually* occurred and how the company has responded to such breaches.

2) **Cybersecurity Risks Should Stand Alone**: Often public companies include cybersecurity risks mixed in with other unrelated risk factors, such as risks of terrorist attacks or natural disasters. The SEC has commented that cybersecurity risks should be broken out separately and stand alone because of the distinct differences between the risk of cybersecurity attacks and the risk of other types of disasters or attacks.

3) **All Material Breaches Should Be Disclosed**: In some cases, a public company has suffered a cybersecurity attack, but has failed to disclose such attack in its public filings. The SEC has issued comments requesting additional information regarding why the public company does not believe the attack is sufficiently material to warrant disclosure, and if such attack is material, then the SEC has requested that the company include the relevant disclosure in its public filings.

Aside from these three main areas, the panel explained that the SEC is interested in greater disclosure regarding the source of cybersecurity attacks that have occurred, e.g., whether the attack is from a competitor, a foreign government or a hacker group. The SEC is also interested in instances in which the company was initially unaware of a data breach, but a third-party brought it to the company's attention. In these cases, the SEC may request disclosure regarding why the company was initially unaware of the breach. The panel hinted that the SEC will issue comments this year related to these additional areas of interest.

Notably, the panel cautioned that a public company's board of directors has oversight responsibility when it comes to cybersecurity, and that federal agencies other than the SEC are also focused on cybersecurity issues.

Based on CorpFin's panel discussion, it appears that increased cybersecurity disclosure is not just the flavor of the month for the SEC. Public companies should be proactive in their disclosure of cybersecurity risks and incidents to avoid receiving a comment from the SEC. Companies should remember that the board of directors has an affirmative responsibility to ensure that the company has adequate cybersecurity protection, procedures and public disclosure in its filings. Keep an eye out this year for new SEC comments related to the SEC's additional areas of interest mentioned above.

Authors

Adam Veness

Cynthia J. Larose, Member / Co-chair, Privacy & Cybersecurity Practice

Cynthia J. Larose is Chair of the firm's Privacy & Cybersecurity Practice, a Certified Information Privacy Professional-US (CIPP-US), and a Certified Information Privacy Professional-Europe (CIPP-E). She works with clients in various industries to develop comprehensive information security programs on the front end, and provides timely counsel when it becomes necessary to respond to a data breach.