MINTZ

Avoiding SEC Comments on Cybersecurity Disclosure

December 16, 2013 | Blog | By Chip Phinney

VIEWPOINT TOPICS

RELATED PRACTICES

RELATED INDUSTRIES

It's been a little more than two years now since the SEC's Division of Corporate Finance issued its **Cybersecurity Disclosure Guidance**. As reported by our colleagues on Mintz Levin's Privacy & Security Matters blog, the SEC continues to pay close attention to the adequacy of corporate disclosure concerning cybersecurity risks and data breaches and has issued related comments to dozens of companies. In particular, CorpFin has asked companies to provide more focused discussions of cybersecurity risks, distinct from other types of risks, and increased disclosure concerning actual data security breaches that have occurred.

In a new post, our colleague Adam Veness discusses some specific examples of CorpFin comments concerning cybersecurity disclosure and offers five tips on how to avoid such comments. Briefly summarized, they are:

1. Evaluate your cybersecurity systems and procedures to understand vulnerabilities.

2. Determine potential risks and impact of a data breach on your business.

3. Plan for preventing cybersecurity risks and mitigating the effects of a potential breach.

4. Disclose in public filings the risks determined in the evaluation, and the scope of the prevention and mitigation plan.

5. Be specific about company risks and the facts surrounding any actual prior breaches in a stand-alone discussion of cybersecurity risk factors.

Authors

Chip Phinney