BRYAN CAVE
A Broader Perspective

Alert

Data Privacy & Security Team

To: Our Clients and Friends

February 14, 2012

Reporting Cybersecurity Risks - New Obligations for Publicly Traded Companies

Most companies are aware that they may be required to report data security breaches to consumers and, in some instances, state attorneys general, the FTC, or HHS. Publicly traded companies should bear in mind that they have to notify another group—their investors.

The Security and Exchange Commission ("SEC") last year offered first-of-its-kind guidance on when companies should report cybersecurity incidents in their disclosure statements.

The guidance, CF Disclosure: Topic No. 2 "Cybersecurity," provides a walkthrough of circumstances in which a company may need to report cybersecurity related matters in their public disclosures. The guiding principle is to disclose incidents that would be considered "material" under disclosure laws and regulations so that investors have important information when making their investment decisions.

As the guidance notes, cybersecurity could be required for inclusion in various sections of the Form 10-K annual filing by public companies. For example, cybersecurity should be discussed in Item 1A as a Risk Factor if cybersecurity is among the most significant factors that make investing in the company risky or speculative. This discussion should be company specific and include a description of cyber risks that are individually, or in the aggregate, material—including a description of the costs and other consequences of incidents. Depending on the circumstances, disclosures related to cybersecurity may also be necessary in Item 7 Management's Discussion and Analysis of Financial Condition and Results of Operations("MD&A") and Item 3 ("Legal Proceedings").

If a cyber incident occurs, such as a data breach, registrants need to account for the breach, and disclose its impact if the breach materially affects business. This accounting should include efforts taken to mitigate the damage caused by the incident as well as evaluate the losses incurred from such things as actual and potential litigation, breaches of contracts, and diminished future cash flow.

If you are the victim of a data security breach, Bryan Cave's Data Breach Hotline offers 24-hour, seven days a week counseling to firm clients. The Hotline may be reached at +1 888 474 9743 in the United States and +1 202 508 6136 internationally. Acting quickly within the first hours of a cybersecurity incident can be instrumental in avoiding many of the costly problems discussed above.

If you would like further information on data privacy or security, feel free to contact Josh James or David Zetoony in Washington D.C., at +1 202 508 6000; or Jana Fuchs in Hamburg at +49 40 30 33 16 136.