Global Data Privacy and Security Team

Bryan Cave's Global Data Privacy and Security Team has responded to hundreds of data security breaches and routinely helps clients, before a breach happens, analyze and improve upon their ability to respond to a breach if (or when) one occurs.

For more information contact:

David A. Zetoony
Partner
david.zetoony@bryancave.com
1155 F Street, N.W.
Washington, D.C. 20004
phone: 202 508 6030

One Boulder Plaza
1801 13th Street, Suite 300
Boulder, CO 80302
phone: 303 417 8530

LaDawn Naegle
Managing Partner
ldnaegle@bryancave.com
1155 F Street, N.W.
Washington, D.C. 20004
phone: 202 508 6046

Chris Achatz
Associate
christopher.achatz@bryancave.com
One Boulder Plaza
1801 13th Street, Suite 300
Boulder, CO 80302
phone: 303 417 8544

For additional information, please visit www.bryancavedatamatters.com

BRYAN CAVE

Cybersecurity Disclosures: At A Glance

In October of 2011, the U.S. Securities and Exchange Commission ("SEC") issued guidance regarding a public company's obligations to disclose cybersecurity risks and cyber incidents (the "Cybersecurity Disclosure Guidance").[1] The Cybersecurity Disclosure Guidance applies to all SEC registrants and relates to disclosures under the Securities Act of 1933 and the Securities Exchange Act of 1934.

The SEC staff acknowledged that no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents. The staff made clear, however, that there are a number of disclosure requirements that might impose an obligation on an issuer to disclose such risks and incidents. The Cybersecurity Disclosure Guidance then identified and discussed certain of those requirements, including disclosures required in risk factors, MD&A, business descriptions, legal proceedings, financial statements and disclosure controls and procedures. The staff stated that as with other operational and financial matters, issuers "should review, on an ongoing basis, the adequacy of their disclosures relating to cybersecurity risks and cyber incidents," with a view to ensuring timely, comprehensive and accurate information that a reasonable investor would consider material. The staff made clear that if a cyber incident occurs, such as a data breach, registrants should be certain to disclose any material impact of the incident on their business operations and explain how they have taken steps to mitigate damage.

Since the original publication of the Cybersecurity Disclosure Guidance, the SEC has remained focused on the implications of cybersecurity on public companies and regulated financial service firms. In 2014 the SEC's Office of Compliance Inspections and Examinations issued a national exam program alert providing a framework for assessing cyber risk and announcing a plan to examine a sampling of registered broker-dealers and investment advisors to review their cybersecurity preparedness. All public companies should evaluate their current disclosures to ensure that they are consistent with the Cybersecurity Disclosure Guidance and should consider implementing a readiness plan to ensure appropriate and timely disclosures in the event of a cyber incident.

85%
The percentage of Fortune 500 companies that identified cybersecurity risk in a SEC filing in 2012 (the year after the SEC issued the Cyber Disclosure Guide).[2]

46%
The percentage of Fortune 500 companies in 2012 that described the extent of cybersecurity risk as "critical," "significant," "materially harmful," or "seriously harmful" to their business operations.[3]

53%
The percentage of global company executives that described insufficient preparation to manage cyber threats as a risk that could have a "significant impact" on their organizations in 2015.[4]

What every public company should do about cybersecurity disclosures:

- ✓ Evaluate the company's procedures for assessing the materiality of cybersecurity matters and implement a regular schedule of ongoing review, perhaps in connection with the company's regular quarterly reporting processes.
- ✓ Determine what disclosure should be made in the company's SEC filings based on the company's exposure to a cybersecurity incident and the materiality of actions being taken proactively by the company to mitigate risk.
- ✓ Review the company's current disclosures and compare those disclosures to peer companies with similar cybersecurity risks and issues.
- ✓ Consider establishing a disclosure readiness plan in the event of a cyber incident. Review the implications for such a plan of active shelf registration statements, share buyback programs and other ongoing securities market activities.
- ✓ Ensure involvement by the board of directors or the risk management committee of the board in the cybersecurity risk assessment and disclosure planning.

[1] Securities and Exchange Commission, CF Disclosure Guidance Topic No. 2: Cybersecurity, Oct. 13, 2011, www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[2] Willis, Fortune 500 Cyber Disclosure Report, 2013, http://www.willis.com/documents/publications/Services/Executive_Risks/2013/FinexNA_Cyber_Update_v2.pdf.

[3] *Id.*

[4] Protiviti, Executive Prospectives on Top Risks for 2015, 2015, http://www.protiviti.com/en-US/Documents/Surveys/NC-State-Protiviti-Survey-Top-Risks-2015.pdf.