JW | Corporate & Securities e-Alert

An important corporate & securities law update from the law firm of Jackson Walker.

January 23, 2012

Resources

JW Corporate & Securities Practice Area

JW Corporate & Securities Attorneys

JW Corporate & Securities Publications

Contact JW

www.jw.com

Offices

Austin
100 Congress Avenue
Suite 1100
Austin, TX 78701

Dallas
901 Main Street
Suite 6000
Dallas, TX 75202

Fort Worth
777 Main Street
Suite 2100
Fort Worth, TX 76102

Houston
1401 McKinney Street
Suite 1900
Houston, TX 77010

San Angelo
301 W. Beauregard Avenue
Suite 200
San Angelo, TX 76903

San Antonio
112 E. Pecan Street
Suite 2400
San Antonio, TX 78205

Gearing up for 2012 Annual Reporting Season: Has Your Public Company Board Addressed Cybersecurity Risk?

By **Orlando Segura Jr.**, **Stephanie Chandler** and **Steve Jacobs**

As companies have migrated toward increasing dependence on digital technologies to conduct their operations, the risks to these companies associated with cybersecurity incidents have also increased. The consequences of a cybersecurity breach are often severe, and can include theft of financial assets or intellectual property, misappropriation of sensitive information, data corruption, and intentional disruption of the operations of a company, to name just a few. These breaches can arise in myriad ways - from intentional attacks perpetrated by sophisticated and organized hackers to accidental misplacement of data by employees within a company's ranks.

Corporate stakeholders, in turn, have placed pressure on lawmakers and the Securities and Exchange Commission to clarify how these risks and their related potential impact on the operations of a registrant should be described within the framework of the disclosure obligations imposed by the federal securities laws. In response, over the past year the SEC has issued guidance that assists registrants in assessing what, if any, disclosures should be provided about cybersecurity matters in light of each registrant's specific facts and circumstances.

In June of 2011, SEC Chairwoman Mary Shapiro issued an official statement stressing that existing disclosure requirements already impose requirements that reporting companies disclose information regarding cybersecurity risk under existing SEC regulations pertaining to disclosure of risk factors, the description of a company's business, disclosure of possible and pending litigation, and Management Discussion and Analysis. More recently, on October 13, 2011, the SEC's Division of Corporation Finance issued detailed interpretive guidance pertaining to each of the requirements outlined in Chairwoman Shapiro's June statement.

Though the October guidance document does not technically create any new SEC requirements, it does provide companies with advice on how to consider cybersecurity issues within the framework of existing disclosure obligations. Specifically, the document lists five areas where specific disclosure obligations may require a discussion of cybersecurity risks and cyber incidents.

Risk Factors

Under Regulation S-K Item 503(c) requirements for risk factor disclosures generally, registrants should disclose the risk of cyber incidents if these issues are among the most significant factors that make an investment in the company speculative or risky. Cybersecurity risk disclosure must adequately describe the nature of

the material risks and specify how each risk affects the registrant. Registrants should not present risks that could apply to any issuer or any offering and should avoid generic risk factor disclosure. Depending on the registrant's particular facts and circumstances, appropriate disclosures may include:

- Description of outsourced functions that have material cybersecurity risks;
- Description of cyber incidents experienced by the registrant that are material, including a description of the costs and consequences; and
- Description of relevant insurance coverage for cyber incidents.

The guidance document reiterates that the federal securities laws do not require disclosure that itself would compromise a registrant's cybersecurity. Instead, registrants should provide sufficient disclosure to allow investors to appreciate the nature of the risks faced by the registrant in a manner that would not compromise their security.

Management's Discussion and Analysis of Financial Condition and Results of Operations (MD&A)

Under Item 303 of Regulation S-K, registrants should address cybersecurity risks and cyber incidents in their MD&A if the costs or other consequences associated with one or more known incidents (or the risk of potential incidents) represent a material event, trend, or uncertainty that is reasonably likely to have a material effect on the registrant's results of operations, liquidity, or financial condition or would cause reported financial information not to be necessarily indicative of future operating results or financial condition. An example of this type of incident would include the theft of material intellectual property that will lead to reduced revenues or an increase in cybersecurity protection costs.

Description of Business

Under Item 101 of Regulation S-K, registrants should provide disclosure in their "Description of Business" if one or more cyber incidents materially affected a registrant's products, services, relationships with customers or suppliers, or competitive conditions. For example, if a registrant has a new product in development and learns of a cyber incident that could materially impair its future viability, the registrant should discuss the incident and the potential impact.

Legal Proceedings

Under Item 101 of Regulation S-K, registrants may need to disclose information regarding material pending legal proceedings involving a cyber incident to which a registrant or any of its subsidiaries is a party. For example, if a significant amount of customer information is stolen in a cyber theft and it results in material litigation, the registrant should disclose basic jurisdictional and factual information about the proceeding.

Financial Statement Disclosures

To the extent that cybersecurity risks and cyber incidents have an impact on a registrant's financial statements, they should disclose these impacts in their financial statements. Registrants should look to Accounting Standards Codification (ASC) for guidance on how to address, for example, costs incurred to prevent cyber incidents, how to ensure appropriate recognition, measurement, and classification of customer payments and incentives to maintain business relationships with customers after a cyber incident, and how to determine when to recognize a liability resulting in losses from asserted and unasserted claims, including those related to warranties, breach of contract, product recall and replacement, and indemnification of counterparty losses from their remediation efforts.

Additionally, for those reporting companies that have previously relied on SAS 70 Audits from their service providers to meet their requirements under Sarbanes-Oxley, contractual requirements

should be updated to require the appropriate reports conducted in accordance with Statement for Standards for Attestation Engagements No. 16 ("SSAE 16") which may be a Service Organization Control ("SOC") 1 Report which addresses to financial controls or a SOC 2 or SOC 3 Report which addresses security, availability, processing integrity, and confidentiality.

Jackson Walker L.L.P has extensive experience guiding clients through **cybersecurity** related issues as well as **advising boards of directors and management on fulfilling their risk oversight responsibilities**. If you have any questions about this e-Alert, please contact

Stephanie Chandler at 210.978.7704 or **schandler@jw.com**
Steve Jacobs at 210.978.7727 or **sjacobs@jw.com**
Orlando Segura Jr. at 210.228.2462 or **osegura@jw.com**

For additional information, please review the following prior publications:

- **Business Leaders Must Address Cybersecurity Risk**
- **The SEC Starts Talking About Cybersecurity**

Please feel free to contact the following partners in our public company practice group if you would like further assistance with this or any other compliance matter:

Austin
Elise Green – 512-236-2028 – **egreen@jw.com**
Michael F. Meskill – 512-236-2253 – **mmeskill@jw.com**

Dallas
Richard F. Dahlson – 214-953-5896 – **rdahlson@jw.com**
Byron F. Egan – 214-953-5727 – **began@jw.com**
Alex Frutos – 214-953-6012 – **afrutos@jw.com**
Jeffrey M. Sone – 214-953-6107 – **jsone@jw.com**

Houston
Mark L. Jones – 713-752-4224 – **mljones@jw.com**
Richard S. Roth – 713-752-4209 – **rroth@jw.com**

San Antonio
Stephanie L. Chandler – 210-978-7704 – **schandler@jw.com**
Steven R. Jacobs – 210-978-7727 – **sjacobs@jw.com**

---

*If you wish to be added to this e-Alert listing, please **SIGN UP HERE**. If you wish to follow the JW Corporate group on Twitter, please **CLICK HERE**.*

JW | JACKSON WALKER L.L.P.

901 Main Street, Suite 6000 | Dallas, Texas 75202