September 15, 2011

Resources

JW Cybersecurity Practice Area

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

The SEC Starts Talking About Cybersecurity

By **Steve Jacobs**

"Securing cyberspace is one of the most important and urgent challenges of our time." With these words in May 2011, Senator Jay Rockefeller, the Chairman of the Senate Commerce, Science and Transportation Committee, and four other Senators, called upon the Chairman of the Securities and Exchange Commission, Mary Schapiro, to develop and publish interpretive guidance clarifying existing disclosure requirements relating to cybersecurity risk. The Senators' letter stated that a substantial number of companies do not report this risk to investors. The Senators referred to a 2009 study by Hiscox, an insurance underwriter, that 38% of Fortune 500 companies made a "significant oversight" by not mentioning privacy or data security exposures in their public filings.

Chairman Schapiro, in the Commission's first official statement regarding the disclosure of cyberattacks, responded on June 6, 2011. Chairman Schapiro stated that existing disclosure requirements already impose a requirement that reporting companies disclose information regarding cybersecurity risk. The first requirement cited by the Chairman was Item 503 (c) of Regulation S-K—Risk Factors—which requires disclosure of past and future cyber attacks or the effects of a cyber attack. The Chairman continued with her view, stating that the description of a company's business required by Item 101 would require disclosure if a company's trade secrets were compromised in a cyber attack; Item 103 could be implicated if there were pending material litigation relating to a company's customer database being attacked causing a release of personal information; and Item 303—MD&A—could also be implicated if the company's trade secrets were compromised resulting in operating costs and/or losses.

According to Chairman Schapiro, additional disclosure is only required if the risk is material which means there is a substantial likelihood that a reasonable investor would consider it important in how to vote or make an investment decision.

While Chairman Schapiro's response does not set forth clear guidelines for disclosing cybersecurity risk, it is clear that companies should begin evaluating this risk to allow them to make an informed decision as to whether they face a material risk associated with cybersecurity.

In August 2010, Jackson Walker published an article titled "**Business Leaders Must Address Cybersecurity Risk**." In that article, we recommended the following:

> Give Cybersecurity High Priority. Cybersecurity should be given a much higher priority level within organizations so that cybersecurity efforts are given an appropriate level of funding given the potential size of the risk. The company's chief technology officer should be required to report to the board or to the

audit or risk committee on a regular basis much like the chief financial officer. All personnel should be appropriately trained and companies should adopt data security policies, document retention policies and internet usage policies such as email and social media policies.

Have a Cybersecurity To Do List. Companies should have regularly scheduled action items concerning cybersecurity. If the company outsources its information technology functions, the board should ensure that the company maintains audit rights, including SAS 70 audits (which allow a company's auditors to rely upon the internal controls of a service organization) of the internal controls of the provider and the contracts should provide adequate definition of the level of security maintained for the data. Even companies that do not outsource, however, must carefully choose vendors and products for their internal systems. For example, when choosing among vendors, leadership needs to consider whether the vendor should have external validation such as FIPS, CIP and PCI DSS compliance. Contract terms should include necessary protections to prevent a cybersecurity breach event and to properly allocate responsibility should a breach occur.

Adopt Cybersecurity Programs. Companies should seriously consider adopting cybersecurity programs. These programs should include certain key elements such as designating an employee who is in charge of compliance; identifying material risks to the company, and the administrative, physical and technical safeguards that are to be applied to protect the confidentiality and integrity of information (such as utilizing virtual private networks or encryption software for transmissions of sensitive data); and continuous testing and monitoring of the program once implemented.

Think About Insurance. Boards may also want to consider purchasing cybersecurity insurance. Often, a company's existing coverage may provide some protection in the event of a cybersecurity breach. New policies are emerging which provide broader coverage for these types of risks. Policies now cover a company's own losses, network related business interruption insurance as well as losses in the event of lawsuits.

To this list, we suggest adding the following:

Disclosure Committees. Disclosure committees should add cybersecurity as part of their process. This will entail including a company's chief technology officer in meetings and discussions.

Risk Oversight. Public companies are required to describe the board's role in risk oversight in their proxy statements including how the board administers its oversight function. In adopting this rule, the SEC explained that "disclosure about the board's involvement in the oversight of the risk management process should provide important information to investors about how a company perceives the role of its board and the relationship between the board and senior management in managing the material risks facing the company." Coupled with the existing internal controls requirements, the effectiveness of a board's risk oversight could be called into question upon the occurrence of a cybersecurity breach which has caused the company damage.

If you have any questions regarding this e-Alert, please contact

Steve Jacobs at 210.978.7727 or **sjacobs@jw.com**. Mr. Jacobs is a partner in the Corporate and Securities Department and Co-Chair of the Cybersecurity practice group of the law firm of Jackson Walker L.L.P. Mr. Jacobs represents both public and private companies including those in the energy, technology and healthcare industries.

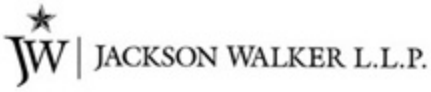
Learn more about Jackson Walker's Cybersecurity practice.

Learn more about Jackson Walker's Corporate and Securities practice.

---

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

Austin Dallas Fort Worth Houston San Angelo San Antonio



Cybersecurity e-Alert is published by the law firm of Jackson Walker L.L.P. to inform readers of relevant information in cybersecurity law and related areas. It is not intended nor should it be used as a substitute for legal advice or opinion which can be rendered only when related to specific fact situations. For more information, please call 1.866.922.5559 or visit us at **www.jw.com**.

901 Main Street, Suite 6000 | Dallas, Texas 75202