ENTERPRISE DATA SECURITY FOR THE SECURITIES LAWYER

STEPHANIE L. CHANDLER, PARTNER
STEVEN R. JACOBS, PARTNER
Jackson Walker L.L.P.
112 E. Pecan Street, Suite 2400
San Antonio, Texas 78205
210.978.7700

The University of Texas School of Law
2013 Conference on Securities Regulation and Business Law Conference – SR13
February 7-8, 2013
Austin, Texas

TABLE OF CONTENTS

ENTERPRISE DATA SECURITY FOR THE SECURITIES LAWYER

Assuring cybersecurity has become a necessity for businesses across all industries. Cybercrime — with over $1 trillion in annual profits — is now the most lucrative illegal global business.[1] Any business with computers and internet access is vulnerable not only from outsiders waiting to pounce but also from within the enterprise as a result of human error or bad intentions. Given the size of this problem, it is not surprising that the National Association of Corporate Directors has stated that to make real progress in the cybersecurity area, businesses must treat cybersecurity as a matter of "corporate best practices" and not just a technology issue.[2] Companies face the risk of substantial damage from loss of customer confidence, decrease in market value and damage to their reputations as well as litigation and regulatory risks in the event of a cybersecurity breach. In October, the Department of Homeland Security sponsored Cybersecurity Awareness Month in an effort to raise awareness and educate Americans about cybersecurity and to increase the resiliency of the nation's cyber infrastructure. Now may be the perfect time for you, too, to refocus on whether your business has adequately planned for the security of its assets.

I. Overview of State and Federal Privacy, Security and Breach Laws

From a regulatory perspective, federal and state laws create obligations on how companies must protect data and maintain cybersecurity. Under federal law, certain industries have heightened obligations as a result of laws such as HIPAA and Graham-Leach-Bliley.[3] In addition, the federal securities laws, including Sarbanes–Oxley,[4] require that corporate leadership maintain adequate controls over their systems which could be implicated upon a cybersecurity breach. Finally, boards of directors of all companies have fiduciary duties to their companies, such as the duty of care, resulting in individual exposure for corporate leadership upon the occurrence of a loss caused by a cybersecurity breach.[5] While this article is focused on the duties of directors, recent Delaware cases have found officers generally have the same duties as directors.[6]

---

[1] *Cybersecurity: Assessing Our Vulnerabilities and Developing an Effective Response: Hearing Before the Committee on Commerce, Science, and Transportation,* 111th Cong. 25–28 (2009) (statement of Edward G. Amoroso, Senior Vice President and Chief Security Officer of AT&T), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-111shrg50638/html/CHRG-111shrg50638.htm.

[2] Four Essential Practices for Information Security Oversight, National Association of Corporate Directors, *available at* http://www.nacdonline.org/Resources/DiscussionGuide.cfm?ItemNumber=1834.

[3] *See* Appendix A.

[4] Sarbanes-Oxley Act of 2002, Pub. L No. 107-204, 116 Stat. 745 (codified in scattered sections of 11, 15, 18, 28, 29 U.S.C.).

[5] *See e.g.*, Byron F. Egan, *Fiduciary Duties of Directors and Officers in Delaware and Texas*, CEO NETWEAVERS DIRECTORS GROUP (Mar. 8, 2012), *available at* http://www.jw.com/publications/article/1715.

[6] *Faour v. Faour*, 789 S.W.2d 620, 621 (Tex. App.—Texarkana 1990, writ denied); *see Lifshutz v. Lifshutz*, 199 S.W.3d 9, 18 (Tex. App.—San Antonio 2006, no pet.) ("Corporate officers owe fiduciary duties to the corporations they serve. A corporate fiduciary is under a duty not to usurp corporate opportunities for personal gain, and equity will hold him accountable to the corporation for his profits if he does so.") (citations omitted). *See generally Zapata Corp. v. Maldonado*, 430 A.2d 779 (Del. 1981); Lyman Johnson & Dennis Garvis, *Are Corporate Officers Advised About Fiduciary Duties?*, 64 BUS. LAW. 1105 (August 2009).

State governments have also been active in legislating protections for data related to consumers and employees residing in their states. Numerous states have made it impossible for a company to shield itself from negative media exposure upon the occurrence of a breach by requiring public announcements regarding the nature and scope of the breach and direct notification of the individuals impacted.[7] In addition to the reactive legislation, many states, such as California,[8] Nevada,[9] and Oregon,[10] have adopted proactive requirements that require businesses to implement and maintain "reasonable" security procedures and practices appropriate to the nature of the information and to protect personal information from unauthorized access, destruction, use, modification, or disclosure. The next wave of regulation arrived in March 2010 when Massachusetts passed a law mandating the development, implementation, maintenance, and monitoring of a "comprehensive, written information security program" for companies that possess data related to Massachusetts residents in order to protect personal information records.[11] Thus, even if you are a business leader with facilities located solely within the state of Texas, if you have customers in one of these states, do business with an independent contractor, or have a sales representative in one of these states, the requirements may apply to your company.

II. Risk Management Responsibility and Governance

While it is impossible to eliminate all risks, there appears to be a serious dearth of board and senior executive oversight over managing cybersecurity risks in the United States. In 2008, Carnegie Mellon CyLab conducted a survey measuring the degree of oversight by boards and senior executives of their organizations' information, software systems and networks.[12] Based upon data from 703 individuals serving on U.S.–listed public company boards, only 36% indicated that their board had any direct involvement with cybersecurity oversight. In addition, only 8% said their boards had a Risk Committee separate from the Audit Committee and, of this 8%, only half oversaw cybersecurity.

A. Public Company Reporting Responsibility

Not attending to cybersecurity risks could result in enforcement action by the SEC as well as private civil litigation. Since 2010, public companies have been 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."[13] 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.

---

[7] *See* Appendix B.

[8] CAL. CIV. CODE § 1798.81.5(b) (2006).

[9] NEV. REV. STAT. § 603A.210 (2006).

[10] OR. REV. STAT. § 646A.622 (2007).

[11] MASS. GEN. LAWS. ch. 93H; 201 CMR 17.

[12] Richard Power, *CyLab Survey Reveals Gap in Board Governance of Cyber Security* (Aug. 22, 2008), *available at* http://www.cylab.cmu.edu/news_events/news/2008/governance.html.

[13] SEC Release Nos. 33-9089; 34-61175, Proxy Disclosure Enhancements (Dec. 16, 2009), *available at* http://www.sec.gov/rules/final/2009/33-9089.pdf.

Title search: Enterprise Data Security for the Securities Lawyer

First appeared as part of the conference materials for the
35th Annual Securities Regulation and Business Law session
"Cyber Security for the Securities Lawyer"