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

I. Overview of State and Federal Privacy, Security and Breach Laws 1
II. Risk Management Responsibility and Governance 2

A. **Public Company Reporting Responsibility 2**
B. **Fiduciary Duty 3**

III. Best Practices 3

APPENDIX A Regulatory Overview 5
APPENDIX B Texas's Amended Data Breach Notification Law Increases Complexity for Businesses 6
APPENDIX C House Passes Cybersecurity Bill Despite Controversy 8
APPENDIX D The SEC Starts Talking About Cybersecurity 9

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.

B. **Fiduciary Duty**

In addition to the federal laws, all directors have a duty of care to their companies under state corporation laws. Under Texas law, the duty of care requires a director to perform his duties with such care as an ordinarily prudent person would use in similar circumstances.[14] Although a director must act diligently and with the level of due care appropriate to the particular situation, the Delaware courts have held that action (or inaction) will constitute a breach of a director's fiduciary duty of care only if the director's conduct rises to the level of gross negligence.[15] Compliance with the duty of care requires active consideration of the issues facing the company. While the standard for proving a breach of duty is high, given the current business environment and the fact that any cybersecurity breach will be viewed with perfect hindsight, directors should insist that they be given information on the company's cybersecurity measures on a regular basis.

III. Best Practices

Given this background, what should boards of directors be doing to fulfill their obligations with respect to cybersecurity? In many ways, the traditional advice to directors still rings true. Directors should attend board meetings regularly; they should take time to review, digest, and evaluate all materials and other information provided to them; they should take reasonable steps to assure that all material information bearing on a decision has been considered by the directors or by those upon whom the directors will rely; they should actively participate in board deliberations, ask appropriate questions, and discuss each proposal's strengths and weaknesses; they should seek out the advice of legal counsel, financial advisors, and other professionals, as needed; they should, where appropriate, reasonably rely upon information, reports, and opinions provided by officers, experts or board committees; and they should take sufficient time (as may be dictated by the circumstances) to reflect on decisions before making them.

However, the very nature of dealing with cybersecurity risks should lead to certain specific actions by directors. Cybersecurity should be given a high 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.

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 SSAE 16 Report SOC 1, 2 and 3[16] audits (which allow a company's auditors to rely upon the internal controls of a service organization) of the internal controls of the provider. Moreover, the third party 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,

---

[14] *Gearhart Indus., Inc. v. Smith Int'l, Inc*., 741 F.2d 707, 719–21 (5th Cir. 1984); *McCollum v. Dollar*, 213 S.W. 259, 260 (Tex. Comm'n App. 1919, holding approved); *see Landon v. S & H Mktg. Group, Inc.*, 82 S.W.3d 666, 672 (Tex. App.—Eastland 2002, no pet.) (quoting and repeating the summary of Texas fiduciary duty principles from *Gearhart*).

[15] *Smith v. Van Gorkom*, 488 A.2d 858, 873 (Del. 1985), *overruled on other grounds by Gantler v. Stephens*, 965 A.2d 695 (Del. 2009).

[16] Replaces the function of a SAS 70 audit.

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.

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.

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.

Companies that are not proactive and argue that the costs of compliance exceed their available resources and budgetary constraints are making a high risk choice. Every organization should at least take initial steps to assess risks and compliance shortfalls and address high-priority risks one at a time. The cost of reacting to a cybersecurity failure could be more than you bargained for.

For more information on Jackson Walker L.L.P.'s Cybersecurity practice, see www.jw.com/cybersecurity.

Appendix A
Regulatory Overview

LEGISLATION	WHO IS AFFECTED?	WHAT DO SECURITY PROVISIONS COVER?	WHAT PENALTIES MIGHT APPLY?
Sarbanes-Oxley Act of 2002	All companies registered with the SEC, subject to public reporting obligatons	Internal controls and financial disclosures	Criminal and civil penalties
Gramm-Leach-Bliley Act of 1999	Financial Institutions	Security of customer records	Criminal and civil penalties
Health Insurance Privacy and Accountability Act (HIPAA)	Health plans health care clearinghouses, and health care providers	Personal health information in electronic form	Civil fines and criminal penalties
California Database Security Breach Information Act (SB 1386)[17]	State agencies, persons, and businesses that conduct business in the State of California	Reporting of breaches of unencrypted personal information	Civil fines and private right of action
Massachusetts General Law (93(H))	Any entity which stores certain data related to a Massachusetts resident	Strict requirements for protecting stored data	Civil fines
Bottom Line	**Significant impact on US private sector**	**Financial customer, health, personal and government information**	**Criminal and civil penalties and private right of action**

[17] One of many state laws that require reporting, amongst other obligations and penalties.

Appendix B
Texas's Amended Data Breach Notification Law Increases Complexity for Businesses

By **Anna Trimble** and **Bill Cobb**, Jackson Walker L.L.P. (August 2012)

On September 1, 2012, Texas's amended data breach notification law passed in June 2011 will go into effect, and residents of all 50 states will potentially feel the effects. Under the amended law, Texas extends the reach of its data breach notification laws beyond Texas borders to all affected "individuals."1

Under the current law, any entity that "conducts business" in Texas and maintains sensitive personal information on its computer network is required to notify any "Texas resident" whose personal information is, or is reasonably believed to have been acquired by an unauthorized user. The types of Texas businesses affected includes most businesses that maintain customer information, as well as virtually any health care-related business. Yet under the new amendment, any such entity conducting business in Texas must notify all affected "individuals" regardless of whether they call Texas home or not. Thus, any entity conducting business in Texas may be required to notify residents of all 50 states in the event of a data breach involving sensitive personal information. However, for affected out-of-state residents who live in states with their own notification requirements (all but four states have their own data breach notification laws), compliance with their own state law satisfies Texas requirements.2

"Sensitive personal information" is defined as an individual's first name or first initial and last name in combination with the individual's social security number; driver's license number or government-issued identification number; or account number or credit or debit card information in combination with a required security code.3 The definition under the Texas statute also includes information regarding an individual's physical or mental health information; the provision of health care to the individual; or the payment for the provision of health care to the individual;4 this information is referred to as "protected health information" or "PHI" in the health care industry, and is also subject to the privacy and security restrictions of the federal privacy statute known as HIPAA. Texas entities subject to HIPAA will have to determine whether they have breach reporting obligations under HIPAA, the Texas statute, or both, since the standards and requirements of HIPAA and the Texas statute are different.

The amendment also increases the penalties for a failure to notify individuals of a data breach from a maximum of $50,000 (under the old law) to $100 per individual per day of failed or delayed notification, not to exceed $250,000 for a single breach.5 A business subject to this regulation is required to provide notice "as quickly as possible," with exceptions made for criminal investigations.6 However, business owners should keep in mind that written proof of cooperation with law enforcement will be required to justify such a delay.

Cyber security is a timely topic. Studies have shown that in 2011, over 174 million records were reported breached.7 The average cost to an organization resulting from a data breach incident is now reported to be upwards of $6.65 million.8 Despite such figures, Congress has yet to enact a law requiring businesses to notify consumers when their personal information has been compromised. Consumers are protected on a state level in 46 of the 50 states as all but Alabama, Kentucky, New Mexico and South Dakota have enacted breach notification statutes to address this growing trend.

Leaving aside the question of whether Congress's interstate commerce power potentially preempts the extraterritorial nature of the Texas law, more practically, the statute does not elaborate on what it means to "conduct business" in Texas. Under a broad reading of the statute, a business headquartered in New Mexico shipping products to consumers in Texas might be required to notify a customer in South Dakota of a data breach, where the personal information was stored in a data-farm in Indiana.

There is also some question of how the broadly worded law might apply to non-U.S. citizens living abroad whose information is stored on the servers of companies conducting business in Texas. Unless the legislature elaborates on what it means to "conduct business" in Texas, the matter will likely be examined and refined by the courts through consequent litigation.

*This issue is likely to remain a potential liability for any entity that has any business dealings in Texas. If you have any questions regarding this e-Alert or how it may affect your business, please contact **Bill Cobb** at 512.236.2326 or **bcobb@jw.com** or **Stephanie Chandler** at 210.978.7704 or **schandler@jw.com** or **Anna Trimble** at 512.236.2381 or **atrimble@jw.com** or **Jeff Drummond** at 214.953.5781 or **jdrummond@jw.com**.*

[1]Tex Bus. & Comm. Code § 521.053(b) (effective September 1, 2012).
[2]*Id.*
[3]*Id.* § 521.002(a)(2)(A).
[4]*Id.* § 521.002(a)(2)(B).
[5]*Id.* § 521.151(a) (current law) and § 521.151(a-1) (effective September 1, 2012).
[6]*Id.* § 521.053(b).
[7]Verizon Risk Team, 2012 Data Breach Investigation Report (2012)
[8]Ponemon Institute, Fourth Annual U.S. Cost of Data Breach

Appendix C
House Passes Cybersecurity Bill Despite Controversy

By: **Anna Trimble**, Jackson Walker L.L.P. (May 2012)

Business executives and national security leaders are of one mind over the need to improve the security of computers that control elements critical to the U.S. infrastructure. But the two groups are divided over the question of who should bear the responsibility for that effort. The cybersecurity debate is complicated by the important fact that most critical elements of the U.S. infrastructure, from the electric grid to the telecommunications system, are privately held. If a U.S. adversary attacked the computer networks that control those systems, the companies that own them would have to take care of the networks themselves. Some security experts have raised questions about whether private industries are up to the challenge of defending against cyber attacks and whether the subject is getting adequate attention from corporate boards and senior executives.

Enter Congress. In April, lawmakers introduced a variety of bills intended to bolster cybersecurity. The main difference among them appeared to be whether the government should require companies to build up their cyber defenses or just encourage them to do so.

However, as the legislation took shape, another controversy emerged and has taken center stage. The new debate is over privacy protections. The new cybersecurity legislation, officially named the Cyber Intelligence Sharing and Protection Act (CISPA), passed the House on a bipartisan vote of 248-168 late on Thursday, April 26, 2012. But amid concerns that the bill does not sufficiently protect individuals' privacy, the legislation ran into a significant pushback at midweek that portends further wrenching adjustments before a final bill can emerge from the Senate.

CISPA allows private companies to voluntarily share information with certain governmental agencies including, among others, the National Security Agency in order to identify and defeat cyber attacks. The information sharing would be voluntary to avoid imposing new regulations on businesses, an imperative for Republicans.

In addition, CISPA would:

- Allow private companies to receive classified digital signatures and other data from U.S. government agencies, including intelligence agencies like the National Security Agency, to help identify malicious Internet traffic.
- Give private companies (particularly, Internet service providers) the right to defend their own networks and their corporate customers — and share cyber threat information with others in the private sector and with the federal government on a voluntary basis.
- Encourage, but not require, private companies to "anonymize" information that they voluntarily share with government and nongovernment entities.
- Grant Internet service providers immunity from privacy lawsuits in which customer information was voluntarily disclosed as a possible security threat.
- Grant Internet service providers and other companies antitrust protection that immunizes them against allegations of colluding on cybersecurity issues.
- Require an independent audit of information shared with the government.

The Obama administration prefers a Senate measure that would give the Homeland Security department the primary role in overseeing domestic cybersecurity and the authority to set security standards. However, the Senate measure is opposed by business groups because of requirements that businesses adopt measures to improve security, steps executives see as burdensome.

The bill now goes, somewhat weakened, into a conference committee, there to be meshed with a new Senate cybersecurity bill, which is expected to be voted on next month. A final bill for the president to sign — or veto — could possibly emerge from Congress sometime this summer.

*If you have any questions regarding this e-Alert, please contact **Stephanie Chandler** at 210.978.7704 or **schandler@jw.com** or **Anna Trimble** at 512.236.2381 or **atrimble@jw.com**.*

Appendix D
The SEC Starts Talking About Cybersecurity

By **Steve Jacobs** and **Stephanie Chandler**, Jackson Walker L.L.P. (September 2011)

"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 cyber attacks, 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.

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 **Stephanie Chandler** at 210.978.7704 or **schandler@jw.com** or **Steve Jacobs** at 210.978.7727 or **sjacobs@jw.com**. Ms. Chandler 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. Chandler represents both public and private companies including those in the biotech, energy, and technology industries. 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.*