JACKSON WALKER L.L.P.

BUSINESS LEADERS MUST ADDRESS CYBERSECURITY RISK

By Steven R. Jacobs and Stephanie L. Chandler

Assuring cybersecurity has become a necessity for businesses across all industries. According to an FBI study in March 2009, cybercrime—with over $1 trillion in annual revenues—is now the largest illegal global business. 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. 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. As October draws near, Cybersecurity Awareness Month sponsored by the Department of Homeland Security may be the perfect time for you to refocus on whether your business has adequately planned for the security of its assets.

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. In addition, the federal securities laws, including Sarbanes–Oxley, or SOX, 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. While this article is focused on the duties of directors, recent Delaware cases have found officers generally have the same duties as directors.

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. In addition to the reactive legislation, many states, such as California, Nevada, and Oregon, 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 of this year with the new Massachusetts requirements for companies that possess data related to Massachusetts residents mandating the development, implementation, maintenance, and monitoring of a "comprehensive, written information security program" in order to protect personal information records. 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 or do business with an independent contractor or have a sales representative in one of these states, the requirements may apply to your company.

While it is impossible to eliminate all risks, there appears to be a gap in board and senior executive oversight over managing cybersecurity risks. 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. 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.

Not attending to cybersecurity risks could result in enforcement action by the SEC as well as private civil litigation. Starting this year, 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.

In addition to the federal laws, all directors have a duty of care to their companies under state corporation laws. Under Delaware law, the duty of care requires a director to perform his duties with such care as an ordinarily prudent man would use in similar circumstances. 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. 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.

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 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.

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.

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.

Steven R. Jacobs is a partner in the Corporate and Securities Department 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. Mr. Jacobs has been named to *Scene in San Antonio*'s "San Antonio's Best Lawyers" and is listed in *The Best Lawyers in America*.

Stephanie L. Chandler serves as the statewide practice leader for the Technology Section for the law firm of Jackson Walker L.L.P. Her practice focuses on assisting clients with securities law compliance and technology contracting. Her clients range from startup companies commercializing innovations in information technology to large private and publicly traded enterprises. Industries she serves include software, health care and life sciences, transportation; and energy. Ms. Chandler is a repeat selection to the "Texas Rising Star" list (2005-2010) and recognized by *Scene in S.A.* as a San Antonio "Best Lawyer" in the area of corporate law.

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