Board Oversight and Cybersecurity: Leveraging Corporate Governance to Manage Cyber Threats

Fred E. Karlinsky, Esq.
Greenberg Traurig

Richard J. Fidei, Esq.
Greenberg Traurig

Benjamin J. Zellner, Esq.
Greenberg Traurig

Editor's Note: Reprinted with permission of the authors & from the July 21, 2018 edition of The Legal Intelligencer © 2018 ALM Media Properties, LLC.

Cybersecurity remains one of the biggest concerns facing the insurance industry. While all levels of operation within an organization are responsible for cybersecurity, recent litigation and regulatory action have demonstrated that the ultimate responsibility for enacting a company's cybersecurity rests with the board of directors. Many boards of directors have had to defend themselves against shareholders alleging that the board's failure to take steps to prevent a data breach violated board members' fiduciary duty of care. Regulators have also stepped up examinations of companies' cybersecurity programs, sometimes reminding directors that cybersecurity is not merely a question for IT personnel, but rather a high-priority issue that must be addressed from the top-down**. To avoid potential litigation or regulatory action, boards should be proactive strive to create company-wide cybersecurity protocols and policies that regularly test cybersecurity systems, require training in cyber risk management, establish a data breach response plan, and implement appropriate oversight of third-party service providers.**

As noted above, a board's duty with respect to cybersecurity is generally to oversee the company's cybersecurity policies, procedures, and strategies, and adequately assess cyber risk, in order to help ensure that appropriate mechanisms have been implemented by management. One oversight strategy is formation of a committee responsible for managing and overseeing the company's cybersecurity systems and IT personnel. This could be the Committee responsible for overseeing the company's risk management policies and procedures, such as a Risk Committee ("RC"). Larger companies may consider formation of an independent Cybersecurity Risk Committee ("CRC") to focus exclusively on cybersecurity, data management, and IT. Whether to form an independent CRC or rely on an existing RC will depend on the size and complexity of the insurer and the sensitivity of the data that the company must safeguard.

The board, through an RC, CRC, or otherwise, should evaluate the company's data management and IT systems to put in motion strategies to help identify vulnerabilities and weaknesses. This analysis will assist in

Read more on page 19

Board... continued from page 9

the establishment of a written Cybersecurity Program ("Cyber Program") that, at a minimum, contains detailed data management and cybersecurity policies and procedures that should be followed by all employees throughout every level of the organization. The Cyber Program should be periodically reviewed by the board or a committee to evaluate its effectiveness and to determine whether improvements are needed. The board should also consider establishing the position of Chief Information Security Officer ("CISO") of the company, who will be responsible for the day-to-day operation of the Cyber Program. The CISO should regularly report to the board or its designated committee to enable the board to adequately oversee the implementation and effectiveness of the Cyber Program.

Adoption of safeguards, such as regular updating and patching of software and continuous monitoring of the company's data network for unauthorized activity, are key functions of the Cyber Program. Additional safeguards should be implemented, as appropriate, to ensure that sensitive data is maintained within the company's secure internal network and is never transferred to unsecured, external networks, such as the Internet, or unauthorized devices such as unencrypted USB drives or CDs unless the proper procedures are followed.

Retention and disposal of data is an often-overlooked component of a company's cyber defenses. The Cyber Program should incorporate data retention policies that dictate the method and length of time data should be retained. Generally, sensitive data should be retained only as long as necessary for the company's business purposes, or for so long as is legally necessary. Procedures must be adopted to ensure that such data is disposed of securely. However, some exceptions to the normal data disposal policies must be incorporated. For example, legal hold policies must be implemented to ensure retention of data that may be subject to pending or threatened legal or regulatory action. Failing to implement legal hold policies could lead to the imposition of civil and possibly criminal sanctions upon the company. Accordingly, it is critical that the designated board committee work with counsel to oversee the implementation of legal hold policies and adopt mechanisms to ensure that such policies are being strictly adhered to.

The Cyber Program should also establish cybersecurity training for employees. Many breaches have resulted from the mishandling of data or communications networks by negligent employees, or by accidentally clicking on a malicious link or attachment. While it is impossible to protect against every risk, the company should provide employees with practical guidance and training to help minimize a company's exposure. It is especially important that training programs be updated regularly to

Fred E. Karlinsky *is Co-Chair of Greenberg Traurig's Insurance Regulatory and Transactions Practice Group. Fred has nearly 25 years of experience representing the interests of insurers, reinsurers and a wide variety of other insurance-related entities on their regulatory, transactional, corporate and governmental affairs matters. Fred is a recognized authority on national insurance regulatory and compliance issues and has taken a leadership position in many insurance trade organizations, has led many industry-driven legislative and regulatory initiatives, and is a sought after thought leader who has spoken and presented to insurance executives and governmental officials, both nationally and internationally.*

Rich J. Fidei *is a shareholder in Greenberg Traurig's Insurance Regulatory and Transactions Practice Group and Government Law & Policy Group in Fort Lauderdale and Tallahassee. Rich focuses his practice on national insurance regulatory, transactional and compliance matters. He represents a wide variety of insurance entities, including insurers, health plans, reinsurers, and other related entities in connection with regulatory, corporate, compliance and transactional issues.*

Jamey Zellner *focuses his practice on government law and policy matters. He is experienced handling a wide range of insurance regulatory and corporate transactions, including company and agent/agency compliance, throughout the country.*

address evolving cyber risks identified by the company. Controls, such as multi-factor authentication and limitations on who within the company may access certain data sets, should also be implemented to ensure that only authorized employees have access to secure networks.

The Cyber Program should also provide for requirements for contracting with third-party service providers to ensure that the company only does business with vendors who have adequate cyber safeguards in place. The company should also implement due diligence protocols to periodically assess the cybersecurity practices of contractors with which the company is doing business.

Incident response plans should also be prepared, implemented, and kept up to date to address new and emerging cyber threats. These response plans outline the procedures to be followed by the company following a data breach to help mitigate damage and make any required notices to consumers, law enforcement, and regulators. Directors should make sure that an emergency response team, sometimes composed of members of the designated board committee, legal counsel, IT personnel, compliance officers, and communications personnel, is in place to respond quickly to a breach. Each member of the response team should have clear roles and responsibilities, such as securing compromised IT assets to spear-heading necessary notices. These measures can help to mitigate any potential liability that results in the wake of a breach.

The board should further oversee the CISO in carrying out periodic testing of the Cyber Program to evaluate its effectiveness. A "penetration test," designed to simulate a real-world cyber-attack, can be conducted by an in-house team or third-party professionals to identify vulnerabilities to be strengthened. Issued revealed by the test, as well as solutions that can be implemented, should be brought to the attention of the entire board and should be addressed as expeditiously as possible with follow-up monitoring to determine whether the issue has been adequately addressed.

Implementing important corporate governance mechanisms aimed at securing the company's data management and IT systems helps develop a culture of compliance in light of new and evolving regulatory requirements. The New York Department of Financial Services ("NYDFS") has taken the lead on establishing new cybersecurity standards with which insurance companies and financial institutions must comply. All insurance company boards should be aware of the requirements of the NYDFS regulation, regardless of whether they operate in New York, because those regulations have been highly influential on other regulators at both the state and

federal levels, who are now taking steps to impose their own new cybersecurity requirements on insurers and financial institutions. Also worth monitoring is the National Association of Insurance Commissioners' recent adoption of the Insurance Data Security Model Law, which has already been adopted by South Carolina and is expected to be adopted by many other states.

Cybersecurity will continue to be a major issue affecting all companies, but especially for insurers that collect and store massive amounts of sensitive policyholder data. Insurance companies may be exposed to legal liability if they fail to implement and oversee cybersecurity protocols in their respective organizations, which could result in board member liability under certain circumstances. Regulators will continue to monitor companies and conduct IT-focused examinations, and may take action if a company has not adopted effective cybersecurity defenses. Effective cybersecurity corporate governance is key to ensuring compliance with regulatory standards, satisfying the board's duty of care, and to avoiding the many negative consequences of a data breach. Boards are therefore well-advised to make cybersecurity concerns a top priority.