Corporate Governance in Insurance: Creating Effective Corporate Governance Mechanisms to Address Cybersecurity Threats



Authors from left to right:
Fred E. Karlinsky
Rich J. Fidei
Christian Brito

Cybersecurity attacks continue to plague companies around the globe. Recent litigation and regulatory action have demonstrated that the responsibility for maintaining a company's cybersecurity rests with the board of directors. In the wake of recent cyber-attacks, shareholders have filed suit against board members, alleging that their failure to take steps to prevent a data breach violated board members' fiduciary duty of care. Regulators have also taken action against companies affected by data breaches, 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. Rather than being compelled to act through litigation or regulatory action, boards should be proactive and create company-wide cybersecurity protocols that would regularly test the company's cybersecurity systems, train its employees in cyber risk management, establish a data breach response plan, and manage relationships with third-party service providers.

The board must also implement appropriate mechanisms to guarantee it can adequately oversee the company's cybersecurity systems and personnel. One effective way of doing so is to appoint a committee that would be responsible for managing and overseeing the company's cybersecurity systems and IT personnel. In the right circumstances, this could be the Committee responsible for overseeing the company's risk management policies and procedures, such as a Risk Committee (RC). Another alternative for certain companies may be to appoint an independent Cybersecurity Risk Committee (CRC) to focus exclusively on cybersecurity, data management, and IT. A CRC would be especially valuable to large insurers that handle significant amounts of sensitive customer and employee data.

Boards should consider the appointment of directors with IT knowledge to sit on the designated board committee.

Expertise is an important factor in selecting committee members. Boards should consider the appointment of directors with IT knowledge to sit on the designated board committee.

To best safeguard company data, the RC or CRC should evaluate the company's data management and IT systems and identify vulnerabilities and weaknesses that could be exploited by bad actors. Armed with that knowledge, the Board should establish a written Cybersecurity Program (Cyber Program) that (at a minimum) contains detailed data management and cybersecurity rules and procedures that must be followed by all employees throughout every level of the organization. The board may also designate a Chief Information Security Officer (CISO), a senior manager responsible for the day-to-day operation of the Cyber Program. By communicating regularly with the CISO, the designated board committee can oversee the effectiveness of the Cyber Program.

One key function of the Cyber Program is the implementation of safeguards, such as regular updating of cybersecurity software and continuous monitoring of the company's data network to detect suspicious activity and possible threats. Additional safeguards should be implemented 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 USB drives or CDs.

All data pathways between the internal network and external networks should be monitored and secured through the implementation of firewalls and similar security measures. Such pathways have become especially important due to the socio-technological phenomena known as the "Internet of Things," where devices such as security

This article first appeared in the Fall 2017 issue of *The Demotech Difference*, a publication of Demotech, Inc., www.demotech.com

cameras, thermostats, printers, and automobiles transmit data over the Internet to other devices.

In addition to implementing procedures designed to maintain the integrity of the company's data networks, the Cyber Program should incorporate data retention policies that dictate the manner in which and the extent to which the company's data should be retained. Generally, sensitive data should be retained only so long as is legally necessary,

The Cyber Program should also establish mechanisms for educating employees on how they can minimize risk.

or for so long as it serves a legitimate business purpose, whichever is longer. Procedures must be adopted to ensure that such data is disposed of safely. Importantly, these procedures must include legal hold policies that would ensure the company retains all data that is or may be the subject of pending or threatened legal or regulatory action. Failing to implement legal hold policies could lead to the imposition of civil and possibly criminal sanctions. 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 mechanisms for educating employees on how they can minimize risk. Many breaches have resulted from the mishandling of data or communications networks by employees. While it is impossible to protect against every risk, the company should provide employees the tools they need to help minimize a company's exposure. One method of doing so is to create employee cybersecurity programs that educate employees on the threat posed by cyber-attacks and train them to follow cybersecurity best practices, such as adequately securing mobile devices, avoiding public Wi-Fi-hotspots, identifying and deleting phishing emails, utilizing adequate passwords, and changing their passwords regularly. It is especially important that training programs be updated regularly to address evolving cyber risks identified by the company. Controls, such as multi-factor authentication, should also be implemented to ensure that only authorized employees have access to the network.

The Cyber Program should also list requirements for third-party service providers to ensure they have implemented adequate internal cybersecurity practices before the company does business with them. The company should also implement due diligence protocols to periodically assess the cybersecurity practices of contractors with which the company is doing business. Such oversight and minimum standard thresholds are especially important if the third-party service provider has access to company data.

The company should maintain, regularly review, and update a post-incident response plan. It should outline the procedures to be followed by the company once a cyber-attack has been discovered so as to allow the organization to quickly and efficiently recover from the attack. Directors should make sure that an emergency response team, 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, from securing compromised IT assets to notifying the appropriate authorities and affected consumers. These measures may mitigate any potential liability that results in the wake of a breach.

The designated board committee should work closely with the CISO to ensure that the Cyber Program is periodically tested to evaluate its effectiveness. A "penetration test," designed to simulate a real-world cyber-attack, can be conducted by an in-house team or can be outsourced to third-party professionals. Any vulnerability revealed by the test should be brought to the attention of the entire board and should be addressed as expeditiously as possible.

Implementing important corporate governance mechanisms aimed at securing the company's data management and IT systems will help the board mitigate cyber risk and potential liability. Importantly, maintaining oversight over a robust cybersecurity program can help

MNBB Studio/shutterstock.com

achieve 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 NYDFS regulation, regardless of whether they operate in New York, because those regulations are indicative of a national movement as regulators on both a state and federal levels are taking steps to impose new cybersecurity requirements on insurers and financial institutions. Perhaps more importantly still, the Cybersecurity Working Group of the National Association of Insurance Commissioners recently adopted a draft of its Insurance Data Security Model Law, which is expected to be rolled out across the states for adoption.

Cybersecurity will continue to be a major issue affecting all companies, but it is a particular concern 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. This could even result in board member liability under certain circumstances. Regulators will continue to monitor companies and may take action if companies do not set up appropriate cybersecurity safeguards. Effective corporate governance is a key to ensuring compliance with these standards, to satisfy the board's duty of care, and to avoiding the many negative consequences of a data breach.

Gorodenkoff/shutterstock.com

Fred E. Karlinsky is Co-Chair of Greenberg Traurig's Insurance Regulatory and Transactions Practice Group. Fred has over twenty years of experience representing the interests of insurers, reinsurers, health plans, managing general agencies, brokers, third-party administrators, claims companies and other insurance entities on their regulatory, transactional, corporate and governmental affairs matters. He is experienced in the formation, licensure and capitalization of insurers, business expansion activities, regulatory examinations, reinsurance and alternate risk transfer mechanisms and many other operational and regulatory issues. Recognized as one of the top insurance lawyers by Chambers and Partners, Fred's extensive knowledge of insurance compliance matters and insurance-related legislative and regulatory initiatives is applicable nationally and internationally. Fred can be reached at 954.768.8278 or karlinskyf@gtlaw.com.

Rich J. Fidei focuses his practice on national insurance regulatory and compliance matters as well as insurance transactional matters. He represents a wide variety of insurance entities, including insurance companies, health plans, reinsurers, producers and other insurance-related entities, in connection with regulatory, corporate, compliance and transactional issues. Rich is experienced in the formation, licensure and capitalization of insurers, business expansion activities, financial and market conduct examinations, reinsurance and alternate risk transfer mechanisms, product filings, as well as many other operational issues applicable to insurance entities. Rich can be reached at 954.768.8286 or fideir@gtlaw.com.

*Christian Brito is a member of Greenberg Traurig's Insurance Regulatory and Transactions Practice Group. Mr. Brito is licensed to practice law only in the Commonwealth of Pennsylvania. *Mr. Brito is not licensed to practice law in the State of Florida and does not practice law in the State of Florida in any capacity. Chris can be reached at 954.768.8279 or britoc@gtlaw.com.*

Additional contribution by: Benjamin Pierce. Mr. Pierce is a member of Greenberg Traurig's Insurance Regulatory and Transactions Practice Group. Mr. Pierce is a graduate of Emory University School of Law. Mr. Pierce is not licensed to practice law in the State of Florida and does not practice law in the State of Florida in any capacity.

Greenberg Traurig, LLP (GTLaw) has more than 2,000 attorneys in 38 offices in the United States, Latin America, Europe, Asia and the Middle East and is celebrating its 50th anniversary. GTLaw has been recognized for its philanthropic giving, was named the largest firm in the U.S. by Law360 in 2017, and among the Top 20 on the 2016 Am Law Global 100. Web: www.gtlaw.com Twitter: @GT_Law.