HOT TOPICS

SIDESTEPPING CYBER LIABILITY: THREE BEST PRACTICES

Directors and officers are facing increased pressure to meaningfully understand, assess, and manage cybersecurity and its associated risks. It is no longer enough for corporate boards to make sure their company's chief information officer or IT department is handling the issue. Instead, directors and officers have a duty to be conversant in information technology, data management, and cybersecurity so they can confirm that proper due diligence is being employed to manage those risks companywide.

A board's failure to drill down on cybersecurity issues may create litigation risk and personal liability exposure, especially if the appropriate insurance coverage is not put in place. Here are three best practices directors and officers should implement to manage cyber risk, as well as to mitigate litigation and personal liability exposure.

1. Cybersecurity and risk management should be "standing" board agenda items. At each board meeting, the board should undertake a detailed review of at least one aspect of cybersecurity risk management.

For example, the board should have a working knowledge of the contingency plan that is in place in the event of a data security breach and should confirm that the response team is qualified, complete, and robust enough to account for the unexpected nonavailability of response team members.

The board should also carefully scrutinize where the company maintains and stores its electronic data. It should examine the company's written corporate policies regarding the handling of electronic data and confirm that procedures are in place to audit compliance, particularly across the employee population.

To the extent outside vendors are used, the board should understand both the vetting process associated with selecting those vendors and the procedures that are in place to monitor changes to the vendor's performance and management team. The board should also be apprised of the company's approach to risk allocation of cyber risk through "standard" company contracts and confirm that the approach is right sized and realistic, e.g., there is likelihood that the indemnification clause will be honored.

2. Conduct a careful audit of the company's insurance program. In the event of a data security breach, one of the first questions that will (or should) be asked is whether the company has insurance coverage available to defray the costs associated with responding to the breach. The board should be out front on this issue by conducting a detailed audit of the company's insurance program before a loss is incurred.

To a large degree, the insurance industry is taking aggressive steps to eliminate coverage for cyber-related risks from "traditional" insurance policies, e.g., general liability, employment practices, D&O, and crime. Cyber coverage is disappearing from those policies mainly through the inclusion of broad, sweeping endorsements that bar coverage for intentional and unintentional disclosure of electronic data. Of particular note, many D&O policies are starting to include exclusions and other policy conditions, such as sublimits designed to significantly scale back the scope of coverage for cyber risks that is available to directors and officers.

Board members need to know, however, that not all traditional policies contain these exclusions, and, in fact, coverage for cyber risks may still exist under those policies. Even more important, board members need to know when those exclusions are being added to the company's policies so they can be sure a premium reduction is secured for the commensurate reduction in coverage.

The board should also determine whether dedicated cyber coverage has been secured, and if not, why not? Dedicated cyber policies are incredibly complex insurance products that offer a variety of coverage grants and are subject to detailed terms and conditions. The board must be sure that proper diligence is conducted for those policies because there are currently more than 40 different cyber insurance policy forms available in the market, and the pricing/negotiability of such policies varies greatly. Consultation with a knowledgeable broker who specializes in the placement of cyber policies along with experienced coverage counsel is also recommended.

3. Careful documentation of the board decision-making process. Managing cyber risks "perfectly" is cost prohibitive. Nevertheless, regulators, shareholders, the plaintiffs' bar, and insurers are expert at questioning the absence of security measures after a breach has occurred. In order to mitigate personal liability exposure and avoid litigation, board members would be well served to document the process of creating, prioritizing, and implementing the cybersecurity "shopping list" used by the board. A written record that demonstrates careful deliberation and reasonable

assessment of deprioritized items will go a long way toward establishing that sound business judgment drove the decision-making process.

Conclusion
Cybersecurity and data management risk exposures will continue to evolve at an alarmingly rapid pace. Directors and officers must remain vigilant in managing those risks through focused board discussion, careful consideration of insurance options, and documentation of board decisions.

Lynda Bennett is chair of Lowenstein Sandler LLP's Insurance Recovery Practice.

SEEN AND HEARD

DIRECTORS PREPARE FOR THE FUTURE AT ANNUAL BOARDROOM SUMMIT

NYSE Governance Services' 12th Annual Boardroom Summit held last month in New York offered nearly 300 attendees a chance to dig into some of the most critical issues for corporate board members today—shareholder activism, executive compensation metrics, regulatory updates, boardroom succession planning, and cybersecurity, to name a few. Experienced directors joined event partners KPMG, Pearl Meyer & Partners, Spencer Stuart, and Wilson Sonsini Goodrich & Rosati for general session panels, which offered unique perspectives, lessons from the trenches, and actionable takeaways for those in the audience.

Kicking off this year's Boardroom Summit was a keynote address delivered by Edie Weiner, founder of The Future Hunters, a consultancy that identifies and analyzes long-term trends that impact businesses. Using newly coined terms such as "effreshancy," "templosion," and "global urbanexus," Weiner offered out-of-the-box perspectives on the future as well as sage advice applicable to every boardroom today.

On the second day, attendees were treated to an address by SEC Commissioner Louis Aguilar, who spoke to directors about the need for effective engagement, resiliency for better risk oversight, and innovation to prepare for global disruptions and the technological evolution.

While the Summit's presentations and speakers offered a wealth of guidance and takeaways for all members, key to the success of this annual event are the networking opportunities made possible by a series of well-organized peer collaborations, as well as workshops designed to drill down into the specific informational needs of audit, compensation, and nominating/governance committee members, along with a session designed specifically for general counsel.

For more highlights and takeaways from this year's Summit, visit nyse.com/governance.