The Board's Role in Cyberrisk Management

by Joshua Gold

Directors and officers have an ever-growing set of responsibilities when it comes to cyber safety for the organization. New laws are being implemented more rapidly, and existing regulatory frameworks are being enhanced to that effect. Protections for investors, depositors, consumers, patients and employees have become a priority for federal and state authorities, including the Securities and Exchange Commission (SEC), Federal Trade Commission (FTC), New York's Department of Financial Services (NYDFS), the California attorney general and other authorities in the United States and around the world.

A recent *Wall Street Journal* poll of 1,000 of the Russell 3000 companies reported that only 15% of boards have a cybersecurity expert. Forthcoming SEC and NYDFS rules are expected to establish a new level of cybersecurity expertise required for corporate managers and directors. Cybersecurity can no longer be delegated to the IT department. Instead, the board's fiduciary duty to supervise the cybersecurity program will become more pronounced, and post-incident litigation more likely. Thus, a fundamental working knowledge of cybersecurity on the board—which these proposed rules directly require—can abate potential liability and loss resulting from cyberrisks.

The rules will also obligate them to disclose in filings what they are doing to increase board cyber knowledge. There are many ways boards can improve their cyber fluency. For one, they can recruit a cyber-knowledgeable board member to lead a committee chartered to oversee the cyber program. However, the next board opening may not be imminent, and the global shortage of cyber-aware candidates who are senior board-ready makes this a near-term challenge. Instead, a board can independently engage a third-party expert to advise its risk or audit committee while it recruits a capable board member—but that may not satisfy regulators that the board itself has added independent "in-house" knowledge.

More immediately, boards can train their members on the basics of cybersecurity in a way that is appropriate to board capacity and perspective. This can be done reasonably quickly through firms that offer board cyber training. The training can then be disclosed in company filings to demonstrate that the company and the board are taking cyber governance seriously and are taking action.

CYBERRISK MANAGEMENT AND INSURANCE PROTECTION

All organizations know that they need plans for pre-breach and post-breach scenarios. While cyber breaches and hacking incidents are a large part of the equation, liability and loss can also spring from other cyber perils, including those related to collection, use, safeguarding, storage and exposure of data.

Indeed, regulators may strike against an organization that is perceived to have lax security or that has made misleading pronouncements concerning the safety and use of data, even if no security event has occurred. This has already occurred in New York, California and at the federal level, resulting in millions of dollars in penalties for smaller organizations. In extreme cases involving Facebook and other large organizations, the damages sought have been far greater.

RISK MANAGEMENT

Reprinted with permission from *Risk Management*.

www.rmmagazine.com

June 2023

Accordingly, boards and senior management must review their activities when it comes to securing systems, using corporate and customer data, making claims about the use of and security around third-party data, and issuing disclosures to investors and regulators regarding the implications of a cyber incident on business operations and revenue.

The new cybersecurity board governance rules speak to boards' oversight of the organization's cybersecurity risk management strategy, which includes how the organization uses insurance in its risk transfer strategy. Insurance coverage must always be part of the discussion before and after a cyber incident. When purchasing insurance, organizations should take the following considerations into account:

- Is the organization purchasing quality insurance from an insurance company not known for contesting insurance claims?
- In light of more stringent underwriting processes, have the insurance applications for purchase and renewal been completed appropriately and accurately?
- Are multiple lines of insurance coverage needed, such as directors and officers (D&O) insurance, dedicated cyber policies, crime insurance, property insurance, business interruption and inland marine coverage?

When making a cyber claim, organizations need to consider the following questions:

- Have all potentially relevant insurance policies been notified in the wake of a serious cyber incident to avoid late notice forfeiture arguments from the organization's insurance companies?
- Has law enforcement been promptly consulted?
- If a cyber policy is implicated, has the organization started coordinating with the insurer to get forensic firms, breach counsel, class action privacy counsel and regulatory counsel to assess legal issues and efforts to protect the organization?
- Are proofs of loss or statements of loss sought within a certain time, and are tolling agreements necessary?
- If ransomware is involved, is it prudent to negotiate with the cybercriminal and would a payment run afoul of the Office of Foreign Assets Control (OFAC) guidance and implicate actors on the specially designated nationals (SDN) list?
- Additionally, are there suit limitation clause issues that need to be addressed, or subrogation-related discussions to hold with the insurance company?
- If dealing with D&O insurance, do directors and officers require separate counsel from the organization?

These issues can be thorny when relegated to a single line of coverage. In today's cyberrisk landscape, a serious incident can easily trigger several policies across different lines of insurance coverage, making the claims process even more challenging.

No organization will be totally impervious to cyberrisks. However, sound cyber governance at the highest levels of an organization can have a number of benefits with far-reaching implications for stakeholders. Board members and senior officers need to understand cyberrisk and the role insurance plays in cyberrisk management, regularly educate themselves on evolving attack vectors, and institute strong corporate governance strategies in this area. With this expertise, organizations will be better positioned to reduce their cyberrisk exposure, limit liability and weather the inevitable cyber incident. R

Joshua Gold is a shareholder in Anderson Kill's New York office, chair of Anderson Kill's cyber insurance recovery group and co-chair of the firm's marine cargo industry group. He is co-author with Daniel J. Healy of *Cyber Insurance Claims, Case Law, and Risk Management*, forthcoming from the Practicing Law Institute. The author would like to thank Scott Corzine, managing director of the cybersecurity, technology risk and privacy practice at CohnReznick, LLP and leader of the company's cyber board training initiative, for his help preparing this article.

RISK MANAGEMENT

Reprinted with permission from *Risk Management*.

www.rmmagazine.com