ALSTON & BIRD

Privacy, Cyber & Data Strategy / Securities Litigation Advisory: Board Oversight and Cyber Breach Response: What Involvement Strikes the Right Balance?

April 9, 2024

Advisories

By: Kimberly Kiefer Peretti, Cara M. Peterman, Lance Taubin

New regulations, including the new cybersecurity disclosure rules published by the Securities and Exchange Commission (SEC), as well as recent regulatory enforcement actions bringing board governance under scrutiny, continue to push boards in the direction of active engagement in their cyber oversight role. But just what does this mean for a board's involvement with a company responding to a significant cybersecurity incident?

On the one hand, boards that are engaged in a particular matter may take a more limited role in the response, including being provided with material details of the event and asking questions to gain comfort in management's decisions and approach.

At the other end of the spectrum, boards can take a much more engaged role by not only participating regularly in calls as the incident unfolds and asking probing questions but also engaging in key response decisions in a way that leans toward engagement in the day-to-day management of the incident, including:

- Encouraging the company to engage specific third-party experts.
- Directing the company on its decisions to take or not take systems offline given the business impact.
- Strongly encouraging the company to interact with customers and employees in a certain way.
- Expressing outright approval of the decision on whether to engage with and pay criminal extortionists.

With the growing pressure to become active and engaged with cyber risk, what involvement satisfies the board's oversight role and strikes the right balance for it and the company?

Board Oversight Role in Cyber Breach Response

As a general matter, at the time of an incident, the board's role is one of oversight: to oversee the company's material risks from the incident, the company's response to the incident, and the likely impact on the company. Boards exercise this role in significant part by becoming informed on the nature and scope of the incident, the company's action/response plan, the status of the investigation, and the company's containment strategies and remediation plan.

The board should receive timely updates on changes in material facts as the investigation into the nature and scope of the incident unfolds. If a third party is engaged by the company in the response—for example, a forensic investigator or law

firm—the third party may report directly to the board on the key facts or risks associated with the incident.

In short, the board's oversight role in the wake of a significant cyber incident is to become informed and remain actively engaged in understanding the event as facts unfold—particularly, by asking probing questions to assess the company's response.

Not every incident a company experiences will or should be escalated to the board. However, with a growing number of incidents resulting in significant legal, operational, and financial consequences to organizations, boards or relevant board-level committees are expected to have a general awareness of the company's incident response plans and protocols, including what types of incidents will be escalated to it, when, and by whom.

Though there should certainly be some level of discretion in the escalation left to management, there should generally be no surprises when a significant incident occurs nor second-guessing management's decision to escalate and the timing of the escalation. It is helpful, if not expected, to have the escalation process documented to avoid such surprises, and the board should be comfortable with the process. When an incident occurs, it is prudent from a regulatory perspective to document when and how the board is informed and updated on a cyber event. By documenting this reporting and any updates, the company can help shield (or mitigate) potential lawsuits, SEC enforcement actions, and shareholder derivative suits.

The Evolving Regulatory and Litigation Landscape

Recent regulations point toward an expanded role of boards in overseeing cybersecurity programs and, particularly, how a board will be engaged to meet these compliance obligations in a significant cyber incident. For example, the recently effective second amendment published by the New York Department of Financial Services (NYDFS) to its Cybersecurity Regulation requires timely reporting of significant cybersecurity events to the senior governing body overseeing the company's cybersecurity program, expecting the board to take a more active role in a cyber incident.

Similarly, under the new SEC cybersecurity disclosure rules, public companies must disclose in their annual report the board's oversight of the company's cybersecurity risks, including any board-level committee responsible for such oversight and the processes by which the board or its relevant committee is informed of such risks. The new SEC requirements for public companies require a registrant to report "material cybersecurity incidents" on Form 8-K within four business days after determining the incident is material. While the new cybersecurity disclosure requirements do not necessarily require board involvement, registrants frequently involve board members (or relevant committee members) when assessing whether and how to disclose a material cybersecurity incident.

In recent years, several enforcement actions and lawsuits have examined cybersecurity controls and board governance. In actions stemming from cyberattacks, the SEC settled numerous cases, which all involved alleged misrepresentations about the company's security controls, the cyberattack, or associated failures to maintain adequate disclosure controls. The SEC also has a pending matter against SolarWinds, bringing civil claims against the company and its chief information security officer (CISO) for fraud and internal control failures relating to allegedly known cybersecurity risks and vulnerabilities in advance of the SUNBURST cyberattack.

These regulatory developments follow a series of shareholder derivative actions alleging claims "on behalf of the company" against officers and directors for purportedly failing to oversee the company's cybersecurity risks, in breach of their fiduciary duties. For example, shareholders of SolarWinds Corporation filed a derivative action (subscription required) against certain of the company's current and former directors following disclosure of the SUNBURST cyberattack, alleging that they failed to implement a system of corporate controls for overseeing the company's cybersecurity risks and that they overlooked purported red flags of cyber threats against the company.

The Delaware Court of Chancery granted the defendants' motion to dismiss (subscription required) the case, based in part on the plaintiffs' failure to plead that the board allowed the company to violate "positive law" and that "absent statutory or regulatory obligations, how much effort to expend to prevent criminal activities by third parties against the corporate interest

requires an evaluation of business risk, the quintessential board function." While the defendants in the SolarWinds litigation therefore successfully avoided liability, as cybersecurity and privacy rules and regulations continue to proliferate, it remains to be seen whether future derivative plaintiffs may have more success.

Challenges in Striking the Right Balance – Board Oversight vs. Management

As heightened expectations for board involvement in cybersecurity matters continue, striking the right balance for board involvement in a cyber breach response is becoming more challenging as the lines are more blurred. At what point does board engagement by asking probing questions, offering insight, and providing suggested strategic direction in the response overstep the lines of day-to-day management of the incident response?

By way of example, board members may participate in daily forensic investigation calls to receive real-time information, but the input they provide may be interpreted as more a "must do" than "may consider." It can also be challenging for a board member who is experienced in either IT or cyber or has experienced a significant cyber matter for another entity to not jump in, question the level of expertise of the company's cyber forensic investigator, and suggest that the company engage a second forensic firm. Second-guessing management's decision to engage a leading cyber forensic investigator may not only blur the line between management and oversight but also lead to conflicting investigatory findings and distract the company from the necessary investigatory and remediation tasks.

Boards can also be tempted to dive into "what went wrong" when the company needs continued focus on what happened to prevent a similar occurrence. Requesting information, investigation, and documentation into "what went wrong" can often not be in the company's best interest, especially in the early stages of responding to an attack.

Of course, there are areas of a company's response where board input and even approval might be expected. In particular, in ransomware attacks, management may seek approval from the board to negotiate and pay a ransom up to a certain amount, if management and the board determine that making payment is in the best interests of the company.

As directors become increasingly educated, experienced and involved in cybersecurity matters, the line between appropriate cyber-risk oversight and day-to-day management is likely to become blurrier.

Board Training and Tabletop Exercises

Tabletop exercises continue to be a useful activity to further develop muscle memory when cyber-attacks occur. To date, most tabletops focus either on the technical aspects of a response, involving the company's information security and information technology teams), or executive tabletop exercises, involving the company's executives from various departments within the company, including not just information security and information technology, but also legal, communications, marketing, finance, human resources, operations, etc.

More recently, boards are becoming involved in tabletop exercises. This could be the result of the recently updated 2023 Director's Handbook on Cyber-Risk Oversight (the "handbook") by the National Association of Corporate Directors (NACD) and Internet Security Alliance (ISA), which stated on page 20 that it "is also advisable for directors to participate with management in one or more cyberbreach simulations, or 'tabletop exercises.'" By including the board (or certain members of the board, such as the members of the board-level committee that oversees the company's cybersecurity program) in tabletop exercises, the board can gain a better understanding of potential cyberattack scenarios, the multitude of issues that arise while responding to a cyberattack, the company's incident response protocols (including how or when the board is notified), and can help board members better understand what their oversight role would look like in an incident response.

Board involvement in tabletop exercises can take many forms. At the outset, it can be helpful for the board to receive a readout following an executive-level tabletop exercise, highlighting the key strengths and areas of improvement for management to focus on moving forward. Once the board understands how management is prepared to respond to an event and the results of its testing of these processes, it can be appropriate to bring the board in.

Companies are conducting training or tabletop exercises directly with board members. These tabletop exercises frequently involve a third-party expert (such as outside breach counsel or a cyber consultant) facilitating the tabletop and walking the board through a simulated cyber incident to allow the board to test their oversight role at key inject points in the incident. For example, by using a scenario involving a ransomware attack that would significantly impact a company's operations, the tabletop exercise for the board would help identify relevant topics where the board would be expected to engage more deeply with senior management, including the remediation and restoration strategy (e.g., when will the company be able to bring back operations?), engaging with the threat actor and whether to make a ransom payment (e.g., would payment accelerate recovery with the decryption key?).

The form of the exercise is often less of a testing exercise and more of a training exercise as the board oversight role should be focused more on becoming informed rather than how to make decisions in the aftermath of an incident.

Practical Tips

While the board's oversight role in cybersecurity is seemingly becoming increasingly complex, there are several tangible steps a board can, and should, take to exercise effective oversight of the company's cyber breach response:

Regular reporting cadence and timely cyber incident communications. Boards should ensure that they are informed of the nature and types of security incidents that are experienced by the company. This includes not only prompt escalation by management to the board for significant cyber incidents but also some sort of regular reporting by management on various types of cyber incidents on a quarterly basis (including those that may not be significant cyber incidents).

Documentation of the board's involvement in incident response . Companies should take steps to ensure that their written incident response plans, processes, or protocols outline the triggers for what type of incidents are escalated to the board (or board-committee), by whom, and when. Without adequate information and an established reporting cadence, the board cannot exercise its oversight role, which could expose the company (and directors and officers) to unnecessary liability. In light of the new SEC cybersecurity disclosure rules, requiring disclosure to the SEC of a "material cybersecurity incident" on Form 8-K within four business days from the date of a materiality determination, companies should also review existing documentation to identify whether, when, and how these determinations are presented to the board.

Develop a relationship and regularly engage with the CISO. Often, the chief information officer (CIO) is the C-suite officer overseeing cybersecurity and the executive directly engaging with the board. While conversations with the CIO are often focused on the discussion of emerging technologies and data capabilities, there is a growing need to bring in the CISO to be part of these conversations and ensure cybersecurity is adequately part of the same dialogue. (See the handbook, page 15.) Regular board engagement with the CISO can help build trust between board members and the CISO, and this trusted relationship can go a long way when responding to a significant cyber incident.

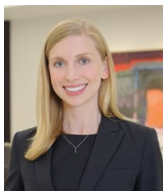
Consider whether the board has the requisite cyber knowledge. While there is no regulatory requirement that board members (or a subset of the board) maintain a specific level of cyber knowledge (the NYDFS decided against including this requirement in its final second amendment to its Cybersecurity Regulation), this skillset could be crucial as cybersecurity tends to be a unique, specialized expertise requiring at least a basic level of cyber literacy to adequately assess and oversee the cybersecurity program. In a promising statistic, in the annual NACD survey of public company directors, 83% of respondents indicated that the board's understanding of cyber risk has significantly improved over the past two years. (See the handbook, page 23). That said, boards should be cognizant of not overly relying on the one director who may have cyber knowledge (when the other directors are not cyber proficient).

Meet the Authors

Kimberly Kiefer Peretti

Partner

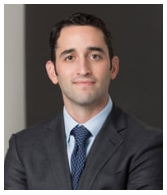
Phone: +1 202 239 3720
Email: kimberly.peretti@alston.com



Cara M. Peterman

Partner

ATL Phone: +1 404 881 7176
NYC Phone: +1 212 905 9196
Email: cara.peterman@alston.com



Lance Taubin

Senior Associate

Phone: +1 212 905 9301
Email: lance.taubin@alston.com