WILMERHALE

Board Oversight of Cybersecurity

MARCH 26, 2018

Cybersecurity is one of the highest priority issues for public company executives and directors. This note shares our views—developed over our involvement in the aftermath of many cybersecurity events as well as counseling on cyber-preparedness—on how boards can properly oversee cybersecurity risks.

First, it is important to note that, last month, the Securities and Exchange Commission—in a much-anticipated release—said that companies should disclose how their boards address the oversight of cybersecurity. Noting the importance of providing investors with sufficient information on the board's role in risk management, the Commission said that a company's required disclosure about how its board administers its risk oversight function should include a discussion of the board's role in overseeing the management of cybersecurity risks where such risks are material to a company's business. The Commission also encouraged companies to address in their disclosure how the board engages with management on cybersecurity issues. In view of this new guidance, more on which can be found here, many companies are including additional information about board oversight of cybersecurity risks in their disclosures, starting with this year's annual meeting proxy statement.

Second, for this and other reasons, we are at an inflection point for boards of directors in assessing how they oversee cybersecurity risks. Here are considerations for boards facing these decisions:

1. **Tailoring Oversight to the Risks**. There are a number of effective models for board oversight of cybersecurity, because cybersecurity poses different risks to different companies. The most effective approach for a given company should be tailored to the business, including the data for which the company is responsible (especially personally identifiable information, such as payment data or health information, as well as key proprietary data and third-party data) and the risks to that data.

2. **Choosing the Right Oversight Structure**. There are several structures that boards have used to oversee cybersecurity risks. The most common choices are to vest responsibility in the Audit Committee, in a Technology or Cybersecurity Committee, in a Risk Committee, or in the Board as a whole. In many companies, the Audit Committee retains primary oversight of cybersecurity risks, consistent with its role in oversight of risks facing the

enterprise generally. In some companies, especially in the financial services sector, primary oversight of cybersecurity is assigned to a Risk Committee that oversees a range of the company's enterprise risks. In still other companies, a designated Technology Committee is tasked with primary oversight of technology-related risks, including, but not limited to, those related to cybersecurity. And finally, in some companies, cybersecurity risks are overseen by the Board as a whole. The differing approaches taken by skilled boards of directors reflect that cybersecurity is not a topic that lends itself to a “one size fits all” model.

3. **The Cadence of Oversight**. No matter where primary oversight of cybersecurity risks is assigned, to be effective, oversight should include regular meetings with the company's chief information security officer. There should be appropriate protocols for elevating information about cybersecurity risks and incidents between those meetings.

4. **Tools for Board Evaluation of Risks**. The committee (or board as a whole) also should consider what measurements to use to evaluate the company's cybersecurity risks and the effectiveness of its controls to address those risks, using appropriate benchmarks to peers and regulatory requirements. Directors will need to decide whether those evaluations should be made by management, internal audit, an external advisor, or some combination over time. The committee (or board as a whole) should have available to it a dashboard—similar to that which is used in Enterprise Risk Management or Audit processes—to look at critical issues, assess how the company is doing, and watch for trends.

5. **Expert Advice**. Boards sometimes ask whether they need to have a cybersecurity expert on the board or on the committee with primary oversight responsibility for cybersecurity risks, akin to the current requirement for financial experts on the Audit Committee. While such expertise can be useful, it is not required, and subject matter expertise should be only one consideration in determining the makeup of an effective board of directors. Indeed, if a board were simply a collection of subject matter experts on each of a company's risks, that would not necessarily be the most effective board of directors. A board should ensure that it has members who are able to converse meaningfully with management and its advisers on this topic, but they need not be cybersecurity experts themselves. Boards and board committees should be able to retain outside expertise to advise them as needed.

6. **Preparation is Key**. A board should assure itself that the company has protocols in place to evaluate and address a potential incident quickly. This usually includes informing itself as to the internal and external resources that the company has engaged to help it in the event of a problem. The board should know that the company has effective internal and external legal, forensic, communications and other expertise to call upon if there is a significant incident.

It is also advisable for the board to understand if management has done incident response planning and periodic tabletop exercises with both internal and external experts to see how it would respond to various potential breach scenarios. The board or committee can hear reports on the results of those exercises and the challenges they may have uncovered. The directors also should ask questions about the company's crisis management policies and protocols and the steps management has taken to implement appropriate disclosure controls and procedures regarding cybersecurity information, including appropriate restrictions on trading by corporate insiders in circumstances in which management is investigating a potential breach.

7. **Red Flags**. As with every area of key risk for a company, directors should ask questions and encourage management to take the time needed to answer them completely, including by involving outside advisers as needed. Directors should be on the alert for red flags, including potential signs that cybersecurity resources are not sufficient or that different or additional personnel are needed. For example, a high level of turnover among cybersecurity personnel could be an issue to discuss with management, and directors should be mindful of reported cyber incidents at peer companies. Directors should respond quickly to any identified red flags, including, where appropriate, by requesting an independent assessment of the health of the company's cybersecurity program.

8. **Management Responsibility**. Obviously, directors should remember that their role is to oversee the company's risk management, not to manage those risks themselves. The board's work should be focused on ensuring that the company identifies its key risks and has adequate policies, procedures, resources, personnel, and organizational structures to manage those risks effectively.

Authors

Jamie Gorelick

PARTNER

Chair, Regulatory and
Government Affairs Department

jamie.gorelick@wilmerhale.com

+1 202 663 6500

Meredith B. Cross

PARTNER

meredith.cross@wilmerhale.com

William R. McLucas

PARTNER

william.mclucas@wilmerhale.com

+1 202 663 6622

Benjamin A. Powell

PARTNER

Co-Chair, Cybersecurity and Privacy Practice

Co-Chair, Artificial Intelligence Practice

benjamin.powell@wilmerhale.com

+1 202 663 6770

Jonathan Wolfman

PARTNER

Co-Chair, Corporate Governance and Disclosure Group

jonathan.wolfman@wilmerhale.com

+1 617 526 6833

Nicole Rabner

PARTNER

nicole.rabner@wilmerhale.com

+1 202 663 6876