April 2016

PRIORITIZING CYBERSECURITY

Five Investor Questions for Portfolio Company Boards

Foreword

As the frequency and severity of cyber attacks against global businesses continue to escalate, both companies and their investors are coming to terms with a grim reality: Data breaches, or cyber incidents, are no longer a matter of if but when. Having put to rest rose-colored notions of eliminating this threat, investors are looking to boards for leadership in addressing the risks and mitigating the damage associated with cyber incidents.

Cybersecurity is an integral component of a board's role in risk oversight. Directors have the authority, capacity and responsibility to make pivotal contributions in this area by ensuring adequate resources and management expertise are allocated to robust cyber risk management policies and practices, and ensuring disclosure fairly and accurately portrays material cyber risks and incidents.

To achieve these objectives, directors need not develop advanced technical expertise. Nor do directors need to support unrestrained capital spending on any project with a "cyber" prefix. Directors need to:

- understand management's cybersecurity strategy;
- learn where cybersecurity weaknesses lie, and;
- support informed, reasonable investment in the protection of critical data and assets.

This publication is intended to help investors communicate one central message: Effective cybersecurity risk management starts with the board. Users should expect companies of various sizes, industries and cyber risk profiles to bring different strategies, in varied stages of implementation, in response to this massive and growing challenge.

Five Investor Questions for Portfolio Company Boards

How are the company's cyber risks communicated to the board, by whom, and with what frequency?

Ensuring that directors are well informed on the company's unique cyber risks is the first, and perhaps most important, step boards can take toward effectively managing this challenge. Although solutions vary, investors should be encouraged by answers that cite regular, not intermittent, board updates.

Not all boards retain outside help for keeping the board fully informed on cybersecurity. In cases where boards rely exclusively on internal resources, investors should feel free to ask about the reason for that approach, carefully consider responses and share their views.

Has the board evaluated and approved the company's cybersecurity strategy?

Boards should evaluate and approve a strategy affirming the company's commitment to minimizing the likelihood that a cyber incident would have a material impact on the business. The strategy should prioritize protecting the organization's most critical data and assets, including data that would result in operational, financial, reputational and legal harm if stolen or damaged during a cyber attack. The strategy should involve not only preventative controls, but also detective and corrective controls. It also should protect sensitive information on how those controls are carried out. Investors should take particular note of whether this strategy:

- reaches as far as the company's third-party business partners, vendors and supply chain, where data security is often most vulnerable;
- recognizes board authority to hire and fire a third party to assess the company's cyber risk management efforts;
- includes thorough incident management procedures;
- clarifies circumstances under which management must inform the board of a cyber incident;
- grants the company's cybersecurity team the authority to nimbly adapt to rapidly evolving and unforeseen cyber threats; and
- includes periodic consideration of whether cyber insurance is a viable, cost-effective risk transfer mechanism.

Investors should expect boards to be familiar with management's incident response plan. For example, is the board confident that management has the right relationships with third-party experts who may need to be tapped to assist with an incident? Similarly,

has the board been briefed on the frequency, and results of, any incident simulation drills conducted by management? Is the board confident that management has a strong communications plan at the ready for when a material cyber incident occurs?

How does the board ensure that the company is organized appropriately to address cybersecurity risks? Does management have the skill sets it needs?

Cyber risk management is an enterprise-wide challenge that cuts across many sides of an organization and many fields of discipline. Investors should look for indications from directors that the company is organized to accommodate this reality. At the management level, companies commonly create cybersecurity working groups involving key executives (e.g. CEO, general counsel, chief financial officer, chief technology officer, chief information officer, and chief information security officer) to set the tactical agenda for identifying and responding to cyber risks.

In addition to the organizational structure, investors should expect that directors have reviewed the backgrounds and qualifications of the management members who are accountable for the company's cybersecurity program.

Ultimately, boards should understand where management-level responsibility and authority have been granted or delegated. Investors should look for a clear delineation of board-level oversight responsibilities in the company's board committee charters and proxy statement risk oversight disclosures.

How does the board evaluate the effectiveness of the company's cybersecurity efforts?

Investors should feel comfortable with boards using their discretion to select cybersecurity performance measures that suit the company's size, industry and cyber risk profile. Investors should look for companies to employ multiple performance criteria spread among broad categories such as:

- rudimentary metrics – measuring the quantity and/or scale of vulnerabilities, attacks and/or incidents detected and/or resolved
- efficiency metrics – measuring the resources expended to detect and/or resolve vulnerabilities, attacks or incidents against an estimate of the damage and/or disruption potentially averted
- compliance metrics – achieving and maintaining compliance with recognized best practices and/or regulatory requirements

Benchmarking against peers may be helpful in measuring cybersecurity performance. Significant disparity with peers may signal that the company's existing strategy is ill-suited to its size or industry, is not being carried out effectively by management or personnel or involves security controls and/or technology that have not been deployed or configured properly. Investors should be encouraged if boards indicate they are

gathering quantitative and qualitative information on how well the company is performing on cybersecurity relative to similar firms, including competitors.

When did the board last discuss whether the company's disclosure of cyber risk and cyber incidents is consistent with SEC guidance?

Investors should welcome indications from directors, and particularly audit committee members, that they are aware of investors' desire for fair and accurate reporting on material cyber risks and material cyber incidents. SEC guidance calls on companies to disclose these risks and incidents, but provides no bright-line test to clarify when disclosure is mandatory. Therefore, it is important for investors to share with boards any concerns they have with narrow interpretations of what constitutes material cyber risk or conservative approaches to estimating the costs of cyber incidents.

Investors will have greater confidence that the company is not withholding information if it proactively communicates the process by which it assesses damage caused by a cyber incident and the methodology it uses to account for cyber incidents affecting data and assets. Communicating such a process will not reveal sensitive information about a company's cybersecurity efforts.