Board Oversight of Cybersecurity Risks

In her regular column on corporate governance issues, Holly Gregory discusses the rapidly changing cybersecurity landscape, and the role of the board in addressing cybersecurity risks to the company.

HOLLY J. GREGORY
PARTNER
SIDLEY AUSTIN LLP

Holly counsels clients on a full range of governance issues, including fiduciary duties, risk oversight, conflicts of interest, board and committee structure, board leadership structures, special committee investigations, board audits and self-evaluations, shareholder initiatives, proxy contests, relationships with shareholders and proxy advisors, compliance with legislative, regulatory, and listing rule requirements, and governance best practice.

The risk of cybersecurity breaches (and the resulting harm) is of increasing significance for most companies and therefore is an area for heightened board attention. In the past several years, more companies have experienced events that compromised sensitive corporate data and confidential customer information, and posed a significant risk to corporate operations. These events ranged from concerted external attacks to lapses in corporate security procedures or employee inattention to those procedures.

Regulators and investors are also focusing on cybersecurity issues. Recent guidance from the Securities and Exchange Commission (SEC), as well as enforcement actions related to high-profile cybersecurity breaches, have sharpened this focus and shed light on regulatory expectations relating to cybersecurity.

The importance of cybersecurity from a broader strategic perspective is highlighted in recent director surveys that identify cyber threats as among the top five drivers of strategic change for companies (PricewaterhouseCoopers LLP, *2017 Annual Corporate Directors Survey*, at 22 (2017), available at *pwc.com*; Nat'l Ass'n of Corp. Dirs., *2017-2018 NACD Public Company*

Governance Survey (2017), available at *nacdonline.org* (login required)). Therefore, boards must understand and be advised on a variety of issues in this complex area, including:

- Common types of cybersecurity breaches and how they can harm a company.
- The board's role in overseeing cybersecurity and the general principles of risk oversight.
- The guidance provided by the SEC, as well as the US Department of Commerce's National Institute of Standards and Technology (NIST).
- How boards can prepare for cybersecurity risks.

CYBERSECURITY BREACHES

Common types of cyber attacks include:

- Unauthorized access to computer systems.
- Inappropriate use of computer systems by current or former employees.
- Installation of viruses or malware on computer systems.
- Social engineering, such as pretexting.
- Theft of private and confidential information.
- Disruption or denial of service.

Cyber attackers may seek to access bank or credit accounts for financial gain, obtain intellectual property or conduct other espionage, or disrupt the company's operations. Notably, 73% of confirmed data breaches in 2017 were perpetrated by outsiders and 50% were carried out by organized criminal groups (Verizon, *2018 Verizon Data Breach Investigations Report*, at 5 (2018), available at *verizonenterprise.com*).

Cybersecurity breaches have the potential to cause significant financial and reputational damage. According to the Ponemon Institute's 2017 *Cost of Data Breach Study* (available at *ibm.com* (login required)), it is estimated that the average total cost to a US company of a data breach is approximately $7.3 million, compared to the global average cost of $3.6 million. In addition to the direct damage caused by a cybersecurity breach, collateral damage may result from:

- Loss of customer confidence.
- Harm to reputation.
- Impact on stock price.
- Potential regulatory action.
- Potential litigation.

The Federal Trade Commission has brought over 130 spam and spyware cases, more than 50 general privacy lawsuits, and more than 60 cases against companies that engaged in "unfair or deceptive practices" that failed to adequately protect consumers' personal data (Fed. Trade Comm'n, *Privacy & Data Security Update: 2017*, at 2-4 (Jan. 2018), available at *ftc.gov*). Settlements may involve consent decrees requiring enhanced information security programs, improved recordkeeping, and annual independent audits for as long as 20 years.

Further, various state unfair and deceptive trade practices laws may support private rights of action. Companies should be aware of state and federal data breach notification laws and the risk of lawsuits for alleged failure to timely notify affected persons of security breaches that involve exposure of personally identifiable information. Cybersecurity failures could also give rise to breach of fiduciary duty, securities fraud, and breach of contract claims, depending on the facts of the situation. Several high-profile cybersecurity breaches have led to enforcement actions against companies and, in one case, civil and criminal insider trading charges against a former executive (Press Release, Dep't of Justice, Former Equifax Employee Indicted for Insider Trading (Mar. 14, 2018), available at *justice.gov*).

GENERAL PRINCIPLES OF RISK OVERSIGHT

In managing and directing corporate affairs, boards have a general obligation to protect corporate assets, including confidential and proprietary information, reputation, and goodwill. This includes overseeing the systems that management has put in place to identify, mitigate, and manage risks to the company's business operations. While recent surveys of directors indicate that cybersecurity is a top concern for boards that some directors feel ill prepared to address, the board's role with respect to cybersecurity primarily relates to risk oversight.

The technical nature of cybersecurity issues may raise concern among directors about whether the board has an appropriate understanding and is providing sufficient oversight. The board need not have a detailed technological understanding of these issues, but the board should be well advised and have access to technological expertise in the management team and advisors.

As in other areas, directors are entitled to rely on management and outside experts on these issues. Ultimately, the business judgment rule presumption should apply to the decisions that directors make regarding oversight of cybersecurity issues, as long as they satisfy the core standards of care, loyalty, and good faith, which apply to board decisions generally.

Directors should apply the same common sense approach to cybersecurity risks that they apply to other business risks. A common sense risk oversight approach should avoid focusing unduly on technical issues. It should instead address issues related to policies and processes, including efforts to educate employees and ensure compliance, and the appropriate deployment of corporate resources.

In general:

- The board should have a high-level understanding of the nature of cybersecurity risks facing the company (which will differ based on the industry and the company).
- The board or a board committee needs to understand and oversee the systems (policies, controls, and procedures) that management has put in place to identify, mitigate, and manage risks related to cybersecurity, as well as respond to cybersecurity incidents.

- The board of a public company needs to provide oversight of related disclosures, as well as disclosure controls and procedures.

LEGAL GUIDANCE

SEC GUIDANCE

The SEC recently released updated interpretive guidance on cybersecurity disclosures (2018 guidance) that reinforces and expands on the SEC's earlier guidance (2011 guidance) (Commission Statement and Guidance on Public Company Cybersecurity Disclosures, SEC Release Nos. 33-10459, 34-82746 (Feb. 26, 2018), available at *sec.gov*).

Under the 2011 guidance, a discussion of cybersecurity risks and incidents may be required in the company's business description or the discussion of risk factors, trends, or uncertainties (in the section of a company's report that provides management's discussion and analysis of its financial condition and results of operations (MD&A)), legal proceedings, financial statements, or disclosure controls and procedures. The 2011 guidance calls on companies to disclose, based on the circumstances and to the extent material:

- Aspects of the company's business or operations that give rise to material cybersecurity risks, and the potential costs and consequences.
- Any outsourced functions that pose material cybersecurity risks and how the company addresses those risks.
- Cybersecurity incidents experienced by the company that are individually, or in the aggregate, material, including a description of the costs and other consequences.
- Risks related to cybersecurity incidents that may remain undetected for an extended period.
- Relevant insurance coverage.

The 2018 guidance:

- Emphasizes that companies should consider the materiality of cybersecurity risks and incidents when preparing required disclosures (in registration statements, periodic reports, and current reports) and warns that an ongoing internal or external investigation would not, on its own, be a sufficient reason to withhold disclosure of a material cybersecurity incident. The 2018 guidance and the accompanying public statements make clear that the SEC and the SEC Staff believe that current company disclosures about cybersecurity risks and incidents should be improved. This is also evident from comment letters issued by the SEC Staff over the past several years that relate to inadequate cybersecurity disclosures.
- Makes clear that a company's disclosure controls and procedures include controls and procedures related to cybersecurity risks and incidents.
- Stresses the need for companies to consider implementing policies to prevent insider trading on the basis of material non-public cybersecurity-related information.
- Notes the implications of cybersecurity incidents for insider trading prohibitions and Regulation FD compliance.

Search Corporate Policy on Insider Trading for a model insider trading policy for a public company that reflects cybersecurity incidents, with explanatory notes and drafting tips.

The SEC voted unanimously in favor of the 2018 guidance, but two SEC Commissioners noted that more can, and should, be done. Commissioner Robert J. Jackson Jr. recently described cyber threats as the "most pressing issue in corporate governance today." Expressing his concern that public companies often err on the side of non-disclosure, Commissioner Jackson urged his colleagues at the SEC to "give careful consideration to new [Form] 8-K requirements governing cyber events." (Robert J. Jackson Jr., SEC Comm'r, Corporate Governance: On the Front Lines of America's Cyber War (Mar. 15, 2018), available at *sec.gov*.) SEC Chairman Jay Clayton also has indicated that the SEC will closely monitor how companies respond to the 2018 guidance and emphasized that its implementation will be a focus of SEC Staff review.

In September 2017, the SEC created a new Cyber Unit of the Enforcement Division to target cyber-related misconduct. Moreover, the SEC's Office of Compliance Inspections and Examinations (OCIE) announced that "[e]ach of OCIE's examination programs will prioritize cybersecurity with an emphasis on, among other things, governance and risk assessment, access rights and controls, data loss prevention, vendor management, training, and incident response" (Press Release, SEC, SEC Office of Compliance Inspections and Examinations Announces 2018 Examination Priorities (Feb. 7, 2018), available at *sec.gov*).

Search Sample Risk Factor: Cybersecurity for a model risk factor relating to cybersecurity that may be included in a public company's annual and periodic reports, registration statements, or private placement offering documents, with explanatory notes and drafting tips.

Search What's Market: Cybersecurity Disclosure 2017–2018 for a discussion of cybersecurity-related disclosures included in recent periodic reports.

NIST GUIDANCE

In addition to general principles of risk oversight, boards should consider guidance contained in the recently revised *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework) (available at *nist.gov*) when addressing the company's risk management and preparedness for cybersecurity events.

The Cybersecurity Framework, which was first released in 2014 by NIST, provides a voluntary framework of standards and best practices aimed at reducing cybersecurity risks to the nation's "critical infrastructure." Critical infrastructure includes physical or virtual systems and assets so vital to the US that their incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these areas. Generally, this includes telecommunications, energy, finance, defense, and transportation companies. While the Cybersecurity Framework was developed to improve cybersecurity risk management in

Boards and their advisors should refer to general principles of risk oversight and the Cybersecurity Framework in engaging management in discussions about cybersecurity issues.

critical infrastructure, it can be used by companies in any sector or community, regardless of their size, degree of cybersecurity risk, or cybersecurity sophistication.

The Cybersecurity Framework is intended to be used by companies to create, assess, and improve a cybersecurity program and provides a common framework for discussing, communicating about, and evaluating cybersecurity functions. The Cybersecurity Framework sets out basic cybersecurity activities that companies should undertake, including:

- Developing an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
- Developing and implementing appropriate safeguards to ensure delivery of critical infrastructure services.
- Developing and implementing appropriate activities to identify the occurrence of a cybersecurity event.
- Developing and implementing appropriate activities to take action regarding a detected cybersecurity incident.
- Developing and implementing appropriate activities to maintain plans for resilience and to restore the capabilities or critical infrastructure services that were impaired through a cybersecurity incident.

The Cybersecurity Framework also includes tools that can be used to assess the degree to which a company's risk management practices exhibit the characteristics defined in the Cybersecurity Framework by categorizing practices into four tiers, which:

- Describe an increasing degree of rigor and sophistication in cybersecurity risk management practices.
- Assist in determining the extent to which cybersecurity risk management is informed by a company's business needs and integrated into its overall risk management practices.
- Support decision-making about how to manage cybersecurity risk, as well as which dimensions of the company are higher priority and should receive additional resources.

The Cybersecurity Framework encourages progression to higher tiers when a cost-benefit analysis indicates a feasible and cost-effective reduction of cybersecurity risk.

While adoption of the Cybersecurity Framework is voluntary, regulators, insurance companies, and the plaintiffs' bar may use it as a reference point in assessing whether a company took steps reasonably designed to reduce and manage cybersecurity risks.

Search The NIST Cybersecurity Framework for more on the Cybersecurity Framework.

ISSUES FOR BOARD CONSIDERATION

Boards and their advisors should refer to general principles of risk oversight and the Cybersecurity Framework in engaging management in discussions about cybersecurity issues. The National Association of Corporate Directors (NACD) and the Center for Audit Quality provide examples of questions directors may pose to management and advisors about cybersecurity, while the Council of Institutional Investors (CII) has published questions for investors to ask portfolio company boards. (See NACD, *NACD Director's Handbook on Cyber-Risk Oversight* (2017) (NACD Handbook), available at *nacdonline.org* (login required); Center for Audit Quality, *Cybersecurity Risk Management Oversight: A Tool for Board Members* (Apr. 2018), available at *thecaq.org*; CII, *Prioritizing Cybersecurity: Five Investor Questions for Portfolio Company Boards* (Apr. 2016), available at *cii.org*.)

The NACD Handbook identifies five steps for boards to enhance their oversight of cybersecurity risks, including:

- Approaching cybersecurity as a company-wide risk management issue, not only an information technology (IT) issue.
- Understanding the legal implications of cybersecurity risks as they relate to their company's specific circumstances.
- Having adequate access to cybersecurity expertise, and giving regular and adequate time on board meeting agendas to discussions about cybersecurity-risk management.
- Setting the expectation that management will establish a company-wide cybersecurity-risk management framework with adequate staffing and budget.
- Discussing cybersecurity risks with management, including which risks to avoid, which to accept, and which to mitigate or transfer through insurance, as well as specific plans associated with each approach.

Directors should also consider the practices of leading companies. PwC, along with *CIO* and *CSO* magazines, recently conducted a survey of their readers and clients, *The Global State of Information Security Survey 2018* (Survey). The Survey reports that board involvement in cybersecurity risk oversight has significant room to grow. For example:

- 44% of respondent directors are "very confident" their company has a comprehensive program to address data security and privacy.
- 39% of respondents are "very confident" their company has identified its most valuable and sensitive digital assets.
- 36% of respondents at companies worth more than $25 billion say their board directly participates in a review of current security and privacy risks.
- 31% of respondents say their board directly participates in a review of current security and privacy risks.

The Survey highlights key actions for data-use governance and reports the extent to which respondents:

- Have an overall information security strategy.
- Require employee training on privacy policy and practices.
- Have an accurate inventory of personal data.
- Limit personal data collection, retention, and access to the minimum necessary.
- Conduct compliance audits of third parties that handle personal data.
- Require third parties to comply with their privacy policies.

(PwC, *Revitalizing Privacy and Trust in a Data-Driven World: Key Findings from The Global State of Information Security Survey 2018* at 9-10 (2018), available at *pwc.com*.)

Risk oversight principles, the Cybersecurity Framework, and emerging best practices suggest that, to be in a better position for active oversight of cybersecurity risks, boards and their advisors should:

- Ensure the board has sufficient information about the company's IT systems.
- Ensure adequate time is reserved on board meeting agendas to discuss cybersecurity issues.
- Consider whether the board needs one or more directors with a sophisticated understanding of cybersecurity issues.
- Determine whether a specialized committee focused on cybersecurity is necessary.
- Periodically review management's assessment of the company's cybersecurity risks.
- Ensure sufficient resources are devoted to the management of cybersecurity risks.
- Ensure sufficient resources are devoted to policies regarding cybersecurity.
- Consider purchasing specific cybersecurity insurance.
- Understand management's crisis preparedness for a cybersecurity breach.

Management should have clearly defined responsibilities relating to cybersecurity risks, and members of the senior management team should be positioned to function in a well-planned and integrated fashion following a breach, including in terms of interaction with regulators, customers, vendors, service providers, and the media.

INFORMATION ON IT SYSTEMS

Board oversight and decision-making relies on information. Directors need to understand the company's IT strengths and weaknesses, and how cybersecurity relates to the company's overall IT strategy and risks and, more generally, to business strategy and risks. This includes discussion of cybersecurity risks where relevant to strategic discussions, which will be more relevant to some companies than others. The board should consider:

- Whether it should receive periodic reports (at least annually and, for some companies, quarterly) on cybersecurity risks, incidents, and activities.
- Whether it has appropriate metrics to assess IT performance, and whether it understands where the company stands in relation to industry practices, as well as whether industry standards are sufficient.
- How to ensure it is adequately informed about the efforts of management to monitor and mitigate associated risks. This includes considering related information and reporting systems designed to keep the board informed.

BOARD TIME AND ATTENTION

The board should reserve time on its meeting agendas to understand and oversee risks associated with the protection of confidential information and intellectual property. In addition, by allocating board time to cybersecurity issues, the board elevates the importance of these issues within the management team and the company. Devoting board attention to these issues underscores that cybersecurity concerns are a priority. Therefore, care should be taken to ensure that adequate time is reserved on board and committee meeting agendas (as appropriate) for review and discussion of cybersecurity issues.

BOARD COMPOSITION

Depending on the complexity and importance of the cybersecurity issues facing the company, the board may consider whether it needs one or more directors with a sophisticated understanding of these issues. Not all companies will require a director with deep technical expertise, but as companies become increasingly dependent on IT and the risks of cybersecurity breaches grow, many boards could benefit from having one or more directors who are sufficiently fluent or are committed to becoming fluent in these areas.

BOARD STRUCTURE

The complexity and importance of cybersecurity issues should be considered in relation to the organization of the board's work through its committee structure. Specifically, the board should determine whether cybersecurity issues warrant particularized attention from a specialized committee. The board also should determine whether the full board or a board committee (such as an audit, risk, or IT committee) has responsibility for oversight of risks associated with cybersecurity. The answers to these questions will differ from company to company.

RISK OVERSIGHT

The board or a board committee should periodically review management's assessment of the risks facing the company related to cybersecurity and management's efforts to monitor and mitigate those risks. This assessment should detail for the board the type and degree of the company's vulnerabilities and should specifically address:

- The most sensitive areas for the company (including vendor, customer, and other relationships).
- The likelihood of a problem, whether through human error or intentional attacks.
- How various scenarios could impact the business.

The assessment should also include a review of the company's cybersecurity strategy, including the policies and practices for managing cybersecurity risks. The board should consider whether the policies and practices are tailored to the company's risk profile, including how they apply to relations with third-party service providers and vendors.

An appropriate board committee should also discuss with management whether cybersecurity risks should be included or expanded in risk factor disclosures, or elsewhere, in annual and quarterly filings (see above *SEC Guidance*).

MANAGEMENT'S ROLE AND RESOURCES

Management is generally responsible for identifying, assessing, managing, and monitoring cybersecurity risks. The board or a board committee should assess the adequacy of resources devoted to the management of cybersecurity issues, and support informed, reasoned investment in the protection of critical data and assets. Management should tailor internal controls, compliance, and education efforts to its assessment of the threats, including the threat of insider failures or malfeasance.

The board should understand how responsibility and leadership regarding cybersecurity issues are structured within the management team and, in this regard, consider whether there is:

- Direct reporting to the CEO or other senior C-level officer (with periodic reporting to the board or a board committee).
- Sufficient coordination at senior levels among business and department leaders.

In particular, the board should decide who in the senior officer ranks has responsibility for information security throughout the organization and the reporting lines. Whether designated as Chief Information Security Officer (CISO) or another title, the position is an important one and should report directly to the CEO, CFO, COO, general counsel, or other senior officer. Changes in this position should be discussed by the board because it will rely on this officer. The position should not be viewed as a "backroom" technical position. The ability of the CISO to lead, communicate, and educate across business and department lines at the senior-most levels of the company is critical.

POLICIES, INTERNAL CONTROLS, AND EDUCATION

The board or an appropriate committee should review the adequacy of resources devoted to policies addressing cybersecurity, related internal controls, and compliance and education efforts. Given that significant risks result from inadvertent as opposed to intentional action, resources and attention devoted to corporate policies and education regarding protection of data and sensitive matters can provide significant benefits.

INSURANCE

The board should discuss with management whether specific cybersecurity insurance is required and whether this insurance is adequate in relation to the costs the company would incur due to a data breach. Regular commercial insurance policies may not cover damages associated with data theft, destruction, or compromise or other harms from cybersecurity breaches.

Cybersecurity insurance may be purchased to cover:

- Event management, including notification costs, public relations expenses, and electronic data loss.
- Business interruption, including lost revenues due to network disruption.
- Cyber extortion, including the costs of investigation and reimbursement of monies paid to ensure continuity of operations.
- Network security and privacy, including the costs associated with defense of claims, investigations, and payment of fines, penalties, and damages.

In addition to providing economic protection should a breach occur, the documentation and audits that insurers require may provide further incentive to put in place appropriate prevention measures, and loss-detection and reporting systems. Moreover, by reducing the financial risk of a cybersecurity incident, insurance may lessen disclosure obligations.

CRISIS PREPAREDNESS

The board should understand how management is prepared for a likely (some would say inevitable) attack or other breach. The board or an appropriate board committee should review with management its plans to address a cybersecurity breach to ensure that the company is well prepared to respond when a problem arises.

Consideration should be given to having a cross-functional incident response team and a cybersecurity incident response plan that engages key IT, compliance, corporate communications, legal, and finance personnel to anticipate common cyber attack scenarios, with preventative and responsive measures tailored to each scenario. Responsibilities for incident response should be clearly defined and understood by the management team, and reporting requirements should be clear, including with respect to which cybersecurity incidents require immediate board notification. The plan should be tested and refreshed periodically.

The views stated above are solely attributable to Ms. Gregory and do not necessarily reflect the views of Sidley Austin LLP or its clients.