© Yoo Jaechang/TongRo Images/Corbis

Board Oversight of Cybersecurity Risks

In her regular column on corporate governance issues, Holly Gregory explores the board's role in addressing cybersecurity risks to the company.

HOLLY J. GREGORY
PARTNER
SIDLEY AUSTIN LLP

Holly counsels clients on the 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.

Last year President Obama issued an Executive Order to help address growing concerns about security breaches relating to confidential information and key computer systems, and the risks that such breaches pose for critical US infrastructure, including infrastructure controlled by a wide range of companies. In October 2013, as directed by the Executive Order, the US Department of Commerce, through its National Institute of Standards and Technology (NIST), issued for comment a set of voluntary standards and best practices intended to help reduce these cybersecurity risks. On February 12, 2014, the final *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework) was released.

The risk of cybersecurity breaches (and the harm that these breaches pose) is one of increasing significance for most companies and therefore an area for heightened board focus. Boards need to understand and be advised on a variety of issues in this complex area, including:

- The different 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 NIST's Cybersecurity Framework.
- How boards can prepare for cybersecurity risks.

CYBERSECURITY BREACH

Breach of a company's data and information systems, whether through inadvertent human error or concerted attack, poses significant risk to corporate operations as well as to critical national infrastructure. In the past year alone, companies have seen a significant increase in events that compromised sensitive corporate data and confidential customer information. These events ranged from concerted external attacks to lapses in corporate security procedures or employee inattention to those procedures. The increased use of mobile devices, social media and cloud computing has increased cybersecurity risks. Further, new developments in communication technologies and their uses tend to outpace the security measures designed to protect information and assets.

As just one example, the growth of the "internet of things," or smart consumer products with internet connectivity, such as automobiles, televisions and even refrigerators, is a development that raises cybersecurity risks in ways that were not anticipated. For example, it has been reported that between late December 2013 and early January 2014, smart appliances (including televisions and at least one refrigerator) were compromised and used to launch a large-scale cyber attack involving malicious e-mails.

Data breaches affect a wide range of industries. According to the *2013 Verizon Data Breach Investigations Report* (Data Breach Report) there is usually a relationship between the industry involved and the motive for the attack. The Data Breach Report found that 75% of reported breaches were driven by a financial motive, such as obtaining bank account or credit account access. Obtaining intellectual property or conducting other espionage is also a significant motive, as is general disruption of the company's or other entity's operations.

The Data Breach Report, which tracked instances of data breaches in 2012, found that:

- 37% of data breaches affected financial organizations.
- 24% of data breaches occurred in retail environments and restaurants.
- 20% of network intrusions involved manufacturing, transportation and utilities.
- 20% of network intrusions involved information and professional services firms.

Notably, the majority of confirmed data breaches were perpetrated by outsiders.

Common types of cyber attacks include:

- Unauthorized access to computer systems.
- Inappropriate use of computer systems by employees or ex-employees.
- Installation of viruses or malware on computer systems.
- Theft of private and confidential information.
- Disruption or denial of service.

Cybersecurity breaches have the potential for significant financial and reputational damage. It is estimated that the average total cost to a US company of a data breach is approximately $5.4 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 40 regulatory actions to date against companies for failures to prevent unauthorized access to consumers' personal information as "unfair or deceptive acts." Settlements may involve consent decrees requiring improved information security programs 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 also need to be concerned with 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 negligence and breach of contract claims, depending on the facts of the situation.

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 many 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 cause a heightened level of anxiety among directors about whether the board has an appropriate understanding and is providing sufficient oversight. Detailed technological understanding is not required by the board, but the board should be well advised and have access to technological expertise in the management team.

As in other areas, directors are entitled to rely on management and outside experts on these issues. Ultimately, the business judgment rule should apply to the decisions that directors make regarding oversight of cybersecurity issues, so long as they abide by 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 not focus unduly on technical issues. It should address issues related to policies and processes, including efforts to educate employees and assure compliance, together with attention to the appropriate deployment of corporate resources.

In general:

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

NIST CYBERSECURITY FRAMEWORK

While the general principles of risk oversight should govern the board's efforts relating to cybersecurity issues, boards may find it helpful to consider the guidance provided by the recently released Cybersecurity Framework when engaging management in a conversation about the company's risk management and preparedness for cybersecurity events.

The Cybersecurity Framework was released by NIST in response to President Obama's Executive Order 13636, titled *Improving Critical Infrastructure Cybersecurity*, which required NIST to develop a new voluntary framework of standards and best practices aimed at reducing cyber 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 and transportation companies.

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 five core functions (Framework Core) and related categories of activities for companies to implement that largely relate to risk management and oversight. The Framework Core includes the following:

- **Identify cybersecurity risks and vulnerabilities.** Companies should develop the institutional understanding to manage cybersecurity risks to organizational systems, assets, data and capability.
- **Protect critical infrastructure assets.** Companies should develop and implement the appropriate safeguards, prioritized through the organization's risk management process, to ensure delivery of critical infrastructure services.
- **Detect the occurrence of a cyber event.** Companies should develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
- **Respond to a detected event.** Companies should develop and implement the appropriate activities, prioritized through the organization's risk management process (including effective planning), to take action regarding a detected cybersecurity event.
- **Recover from a cyber event.** Companies should develop and implement the appropriate activities, prioritized through the organization's risk management process, to restore the capabilities or critical infrastructure services that were impaired through a cybersecurity event.

The Cybersecurity Framework also includes tools that can be used to assess an entity's cybersecurity compliance by categorizing practices into one of four tiers, ranging from partial compliance to adaptive compliance, and to help a company identify steps to achieve their target cybersecurity profile.

While adoption of the Cybersecurity Framework is voluntary, it will likely become a key reference for regulators, insurance companies and the plaintiffs' bar in assessing whether a company took steps reasonably designed to reduce and manage cybersecurity risks.

ISSUES FOR BOARD CONSIDERATION

Boards and their advisors should refer to the general principles of risk oversight and the Cybersecurity Framework in engaging management in discussions about cybersecurity issues. They should also consider recent research about the practices of leading companies.

PricewaterhouseCoopers LLP along with CIO and CSO magazines recently conducted an online study of their readers and clients, titled *The Global State of Information Security Survey 2014* (Survey). According to the Survey, companies that detected more security incidents and reported lower average financial losses per incident, shared the following key attributes:

- They had an overall information security strategy.
- They employed a chief information security officer (CISO) or equivalent who reported to the CEO, CFO, COO or CLO/ general counsel.
- They had measured and reviewed the effectiveness of the company's security measures within the past year.
- They understood what types of security events had occurred in the past year.

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 information technology (IT) systems.
- Ensure adequate time is reserved on the board agenda 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.

It is particularly critical that management have clearly defined responsibilities relating to the management of cybersecurity risks, and that members of the senior management team are positioned to function in a well-planned and integrated fashion, including in terms of interaction with regulators, customers, vendors, service providers and the media, in the immediate aftermath of a breach.

INFORMATION ON IT SYSTEMS

Information is the predicate on which board oversight and decision-making rests. 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 IT and cybersecurity risks where relevant to strategic discussions, which will be more relevant to some companies than others. The board should consider:

- Whether it is appropriate to receive periodic reports (at least annually and, for some companies, quarterly) on cyber risks, incidents and activities.
- Whether it has appropriate metrics to assess IT performance and whether it has an understanding of 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 giving consideration to related information and reporting systems designed to keep the board informed.

BOARD TIME AND ATTENTION

The board needs time on its agenda to understand and oversee risks associated with the protection of confidential information and intellectual property. In addition, by allocating board time to these issues, the board elevates the importance of IT issues and cybersecurity within the management team and the company. Quite simply, attention by the board underscores that IT and cybersecurity concerns are a priority. 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 IT and cybersecurity issues facing the company, the board may wish to 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 ever more dependent on information technologies 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

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

RISK OVERSIGHT

The board or an appropriate 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.

It should also include a review of policies and practices for managing cybersecurity risks and determine whether they are appropriately 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 Form 10-K and 10-Q filings (see *Box, Disclosing Cybersecurity Risks: SEC Guidance*).

MANAGEMENT'S ROLE AND RESOURCES

Management is generally responsible for identifying, assessing, managing and monitoring IT and cybersecurity risks. The board or an appropriate board committee should assess the adequacy of resources devoted to the management of IT and cybersecurity issues. 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 IT and cybersecurity issues are structured within the management team and, in this regard, consider whether there is:

- Direct reporting to the CEO or other very senior c-level officer (with periodic reporting to the board or an appropriate 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 CISO or some other title, the position is an important one and should report directly to the CEO, CFO, COO, general counsel or other very senior officer. Changes in this position should be discussed by the board since 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.

Disclosing Cybersecurity Risks: SEC Guidance

In October 2011, the SEC's Division of Corporation Finance issued guidance on disclosure obligations relating to cybersecurity risks and incidents. Depending on the circumstances, a discussion of cyber risks and cyber incidents may be required in the company's business description and/or in the discussion of risk factors, trends or uncertainties (in the MD&A), legal proceedings, financial statements and/or disclosure controls and procedures.

The SEC's guidance calls on companies to disclose, based on particular facts and to the extent material:

- Aspects of the company's business or operations that give rise to material cyber risks and the potential costs and consequences.
- Any outsourced functions that pose material cyber risks and how the company addresses those risks.
- Cyber 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 cyber incidents that may remain undetected for an extended period.
- Relevant insurance coverage.

Since 2011, the SEC staff has issued comments to dozens of large companies regarding their cybersecurity disclosures, often in response to news articles about cyber risks or an attack on the company or within an industry. These comments tend to focus on:

- Additional disclosure about cyber risks as distinct from more general risks, such as natural disasters or terrorist attacks.
- Disclosure of cyber attacks the company has experienced or an explanation of why they are not material.
- Description of cyber attacks experienced by third-party vendors that may affect the company's customers.

In May 2013, in response to a letter from Senator Rockefeller urging the SEC to require more detailed disclosure, SEC Chairman White asked the SEC staff for a review of current cybersecurity disclosure practices and for recommendations about whether further action is needed.

Search Sample Risk Factor: Cyber Security for a form of risk factor relating to cybersecurity that may be inserted into a public company's annual and periodic reports, registration statements or private placement offering documents.

POLICIES, INTERNAL CONTROLS AND EDUCATION

The board or an appropriate committee should also review the adequacy of resources devoted to policies addressing IT and 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 to the company that would result from a data breach. Regular commercial insurance policies may not cover damage 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 assure continuity of operations.
- Network security and privacy, including the costs associated with defense of claims, and payment of settlement 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 cyber 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 an 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 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.