Nasdaq

Simpson Thacher

Ten Questions Every Board Should Ask in Overseeing Cyber Risks

June 2017

Nasdaq Corporate Solutions | MeetX Board Portal for Meeting Management

Ten Questions Every Board Should Ask in Overseeing Cyber Risks

June 2017

Those who work in the cybersecurity industry believe that there are two types of companies in the United States: "those that have been hacked and those that don't know they've been hacked."[1] Indeed, more and more companies are experiencing data breaches, and it seems that hardly a week goes by without a data breach reported in the headlines.

The consequences of such a breach could be significant. Predictably, a data breach is typically followed by a slew of lawsuits, including putative consumer class action lawsuits and shareholder derivative actions filed against the directors and officers of the company for their alleged breach of fiduciary duties. In recent years, for example, dozens or even hundreds of lawsuits have been filed against certain companies in the retail and healthcare spaces in connection with data breaches. Additionally, various government agencies, on both the federal and state level, have investigated companies for data breaches, and such investigations have resulted in enforcement actions and, consequently, settlements (some of which have been significant). Moreover, data breaches could have a substantial impact on the company's business. The disclosure of a data breach could lead to a meaningful drop in the company's stock price and, as seen in recent months, can reduce the purchase price of a target company significantly. Finally, there is often an incalculable but very real reputational cost to companies that have suffered a data breach. This cost can far surpass the monetary amount paid to settle any lawsuits or regulatory actions.

The costs of a data breach can be exponentially greater where the board is perceived not to have taken the appropriate steps to properly oversee the company's cybersecurity. These added costs include diminished chances to be able to dismiss a shareholder derivative action filed on behalf of the company, as well as negative vote recommendations from proxy advisory firms against the company's directors.

Because of the costs associated with a data breach and the fact that no company today is immune from them, it is essential that each board ensure that it is adequately overseeing the company's cyber risks. Especially for directors who do not have a technology background, this mandate can be a daunting task. The good news, however, is that Delaware sets a very high threshold for finding that directors breached their duty of care; as articulated in the seminal case In re Caremark, while directors have a duty to oversee corporate risk, they are only liable if plaintiffs can demonstrate "sustained or systemic failure of the board to exercise oversight – such as an utter failure to assure a reasonable information and reporting system exists." Recognizing that directors can protect themselves from liability by taking an active oversight role in their company's cybersecurity preparedness, this article sets out to provide boards with some practical advice regarding how to approach cybersecurity oversight and outlines specific categories of questions directors may wish to consider asking to fulfill their oversight duty.

[1] Nicole Perlroth, "The Year in Hacking, by the Numbers," N.Y. Times, April 22, 2013.

A Practical Approach: Ten Questions Every Board Should Ask in Overseeing Cyber Risks

The overriding principle for any board overseeing cyber risks is that cybersecurity should be approached as an enterprise risk management ("ERM") issue, rather than a technological problem for the information technology team to handle. The management of cyber risks is just one element of the company's risk management and oversight, and overseeing such risks should be part of the board's oversight of the execution and performance of the company's ERM program (or, if the company doesn't have an official ERM program, the company's risk assessment and mitigation activities). Accordingly, while directors may not understand all the technological details surrounding data protection systems and processes, the board nevertheless needs to ensure that it is comfortable that management is effectively managing the company's cyber risks, as with any other risk the board oversees through the ERM process.

Fundamentally, to fulfill its duty of care in overseeing cyber risk under Caremark, the board must allot regular and adequate time on its agenda to discuss cybersecurity matters. At a minimum, the board should meet with the person in charge of organization-wide data privacy and security (such as the Chief Information Security Officer) on an annual basis. Similar to other risks the board oversees, the board should spend this time to ensure that it gains a solid understanding of, among other things:

- The cyber risks the company faces, including the potential impact of those risks on the company's business.
- The steps management is taking to mitigate those risks.
- How the company is prepared to handle a security breach.

In practice, ensuring that the company is adequately managing its cyber risks can be difficult. To be better prepared – and to ensure that it is properly fulfilling its oversight role – the board should ask thoughtful questions. While there is no "one size fits all" approach to questions a board should ask in its oversight of cybersecurity (particularly as different industries exhibit different risk profiles), we suggest ten categories of questions that boards of all companies should be asking members of management responsible for cybersecurity. In each case, directors should assess the responses to these questions and determine whether follow-up is required. Additionally, depending on the circumstances, additional questions may be necessary.

1. Leadership

Has the company identified a senior person with clear responsibility for organization-wide cybersecurity preparedness, who has support from the top of the organization?

As with any important management function, someone needs to have ultimate responsibility for cybersecurity. This person is often (but need not be) the Chief Information Security Officer.

2. Budget and Staffing

Has management given serious consideration to how much of the budget and how much staff is adequate for proper cyber risk management?

The appropriate budget and staff will depend on a variety of factors, including the industry in which the company operates. Companies in the healthcare and financial services industries, for example, tend to experience more data breaches than companies in other industries, such as construction or real estate. The board's role is to ensure that management is thoughtful regarding its allocation of resources to cyber risk, given the company's industry and circumstances. Additionally, the board should ask questions to ascertain whether management is properly prioritizing the allocation of funds within the overall cyber budget in accordance with relative risk.

3. Comprehensive, Written Cybersecurity Program

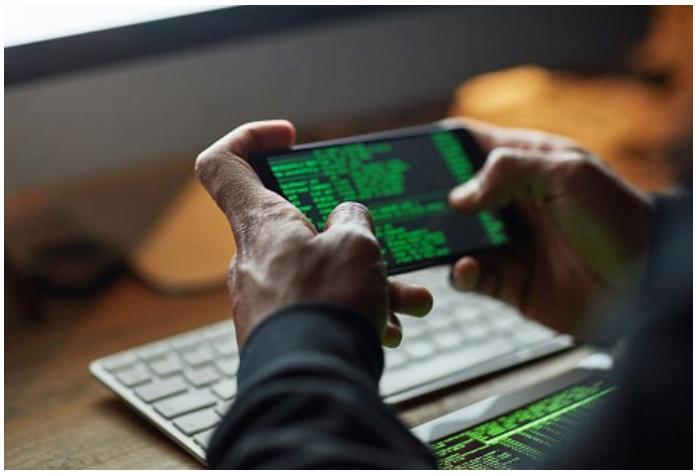
Has management formulated a comprehensive, written data privacy and cybersecurity program consisting of reasonable and appropriate policies and procedures?

It is essential that companies formulate a comprehensive, written data privacy and cybersecurity plan that is reviewed by and distributed to all individuals who may be involved in its execution.

a. Prerequisites to Formulating a Comprehensive, Written Cybersecurity Program

In order to create a robust cybersecurity program, management must first:

- Know where its data resides and who is accessing it.
  - Without this basic information, management will encounter significant hurdles in adequately safeguarding the company's sensitive data.
- Understand the company's top cyber risks.
  - Without knowing what the company's specific cyber risks are at any point in time, management cannot take effective steps toward preventing a breach (or at least mitigating known risks) and cannot allocate its budget appropriately. While many think of data breaches as being synonymous with hacking or cyber-attacks, companies often encounter other types of cyber risk, which could be significant. A prime example is misuse of information by current or departing employees. According to Verizon's 2017 Data Breach Investigations Report, 25% of all data breaches occurred because internal actors abused the access with which they were entrusted – whether maliciously or not (e.g., ignoring protocol or circumventing procedures to facilitate or expedite certain processes). Moreover, even cyber-attacks are multi-faceted and require an understanding of their different phases, each of which generally corresponds to different potential vulnerabilities of the company.



ACCORDING TO VERIZON'S 2017 DATA BREACH INVESTIGATIONS REPORT, 25% OF ALL DATA BREACHES OCCURRED BECAUSE INTERNAL ACTORS ABUSED THE ACCESS WITH WHICH THEY WERE ENTRUSTED – WHETHER MALICIOUSLY OR NOT.

- Know whether there are industry standards applicable to the company's industry and what market practice is among the company's peers in the same industry.
  - Benchmarking could be an important step in ensuring that the company's cybersecurity program is appropriately robust. In this regard, a company may choose to engage an outside advisor that can provide benchmarking services, comparing the company's data security processes and practices with those of its peers.

The board should ask questions to confirm that management has adequately gathered and addressed all of this information in formulating its cybersecurity plan. Given that this information can change over time, the board should make sure to revisit these questions at least annually. The board should also inquire whether and how management got comfortable with the fact that its plan is state-of-the-art.

b. Key Elements of a Comprehensive, Written Cybersecurity Program

Naturally, cybersecurity programs will differ, depending on the company and its industry. There are, however, several hallmarks of any comprehensive cybersecurity program. It must:

- Ensure that the company does not collect or store non-essential customer data.
  - Sensitive information should be retained only as long as the company has a business reason for it. The rationale behind this is simple: If the data is not in the company's system, it cannot be stolen.
- Indicate how the company ensures that data is destroyed responsibly after it has outlived its business purpose.
- Ensure that more sensitive data is stored separately with higher safeguards.
- Ensure that employees are granted access to sensitive data only if necessary for them to perform their duties.
- Indicate the measures the company takes to protect against the downloading of malicious data.

- Indicate what measures the company takes to reduce the risk that data will be transferred from the company's internal network to the outside internet (e.g., implementing a firewall between the company's internal systems and the internet, blocking particular internet connections known to be used by hackers or creating a list of approved servers to which the company's network is permitted to upload).

The board should ask thoughtful questions regarding each of these and any other significant aspects of the company's cybersecurity program.

c. Reassessing and Testing the Cybersecurity Program

The cybersecurity plan must be reviewed with critical eye at least annually, given that the nature and scope of cyber risks are in a constant state of evolution. The board should ask whether the plan has been reassessed and whether changes should be or have been made to the plan as a result.

Moreover, the cybersecurity plan must be tested to gauge its effectiveness. Some companies conduct such testing in-house, while others hire independent third parties to do so. In addition to inquiring as to whether the company's cybersecurity plan has been tested, the board should ask what the results of that test were and how the vulnerabilities identified during such assessment, if any, have been addressed.

4. Employee Training and Education

Has management instituted effective training programs that instruct employees on the appropriate handling and protection of sensitive data?

As with other forms of employee training, cybersecurity training programs should be meaningful, consisting of more than written policies that employees are required to review and sign. The board should ask probing questions to determine whether management has been adequately conveying to employees the company's protocol, the importance of following it and the consequences of not following it. The board should ensure that it is comfortable that management's training and education programs are properly designed to enable employees to internalize the company's cybersecurity policies. The board should also ask questions designed to ascertain whether management is fostering a culture of compliance with the company's data security policies and protocols and holds accountable those who are not compliant with them.

5. Third-Party Vendors

Has management taken steps to mitigate the cybersecurity risks associated with outsourcing business functions to third parties?

According to the 2016 Soha Systems Survey on Third Party Risk Management, 63% of all data breaches were linked to a third party. This statistic underscores that even if a company has a state-of-the-art cybersecurity program, that program is worthless if the company's vendors, who have access to the company's network and/or sensitive data, do not have similarly robust data security policies and practices. In other words, a company's cybersecurity program is only as strong as the weakest link in its vendor chain.

ACCORDING TO THE 2016 SOHA SYSTEMS SURVEY ON THIRD PARTY RISK MANAGEMENT, 63% OF ALL DATA BREACHES WERE LINKED TO A THIRD PARTY.

There are several crucial steps companies should take with regard to their third-party vendors.

- Management should ensure that the company's third-party vendors are aware of the company's information securities policies and agree to adhere to them.
- Prior to entrusting a third party with sensitive data, management should review the third-party vendor's data security policies and ask the vendor specific questions about its data security practices to ensure that the vendor properly handles and secures shared sensitive information.
- Management should make sure that any agreement with a third party clearly identifies:
  - how the service provider will safeguard the organization's sensitive data;
  - whether the vendor will subcontract any services to other vendors and, if so, how minimum data security standards will be set; and
  - whether the service provider will notify the company in case of a breach.
- It is critical that companies properly segment the parts of their network accessible to vendors and those that house sensitive data to which the vendors do not need access.

With these points in mind, directors should ask the appropriate members of management thoughtful questions to ensure that the company is doing all it

can to safeguard the sensitive information to which its third-party vendors have (or could get) access.

6. Legal Compliance and Regulatory

Does management has an effective system in place for staying abreast of and complying with evolving federal, state and international data security laws and regulations that are applicable to its operations?

Those charged with ensuring the company's data security must be aware of any federal, state and/or international laws that require them to take measures to secure sensitive data. Relevant regulations can change with some frequency, and management must have an effective system in place to track such changes and comply with all regulations. For many companies, this undertaking may entail using an outside vendor. The board should assure itself that management has an effective process for staying updated with regard to applicable legal and regulatory changes.

7. Insurance

Has management given serious consideration to purchasing cyber liability insurance?

In today's environment, management should at least give serious consideration to investing in cyber liability insurance. The board should ensure that management has explored whether it makes sense for the company to purchase cyber liability insurance and should ask questions to understand management's approach to purchasing such insurance. If the company has not purchased cyber liability insurance, the board should make sure that it is comfortable with management's rationale for its decision. If the company has cyber liability insurance, the board should ask about its terms and scope of coverage in an effort to ensure that it is sufficient given the company's specific facts and circumstances.

8. Detection

Has management installed adequate technology not only for preventing the downloading of malicious software but also for detecting and alerting the organization to attempted breaches?

It is essential that every company have robust security software tools and antivirus systems in place to detect attempted breaches. But this alone is not sufficient. Each company must also train security employees on the protocol for responding to automated alerts generated by this technology. If a company has systems

that generate alerts but does not have personnel sufficiently trained in handling those alerts, the alerts are not worth much. Accordingly, directors should ask questions to help them understand and assess the measures management has implemented to detect breaches and train employees to respond to breach alerts. Among other things, directors should ask whether any data breaches or incidents have been detected in the past, how long it took for such breaches or incidents to be detected and how their detection was handled by the company's personnel.

9. Comprehensive, Written Breach Response Plan

Does management have a comprehensive, written breach response plan in place?

It is critical that companies be prepared to respond to a breach quickly, effectively and calmly. To that end, companies must have a comprehensive, written breach response plan in place and be clear on what events will trigger that response plan. As part of their response plan, companies should:

- Form a breach response team composed of individuals from key departments (including Information Technology, Legal and Corporate Communications) and identify individual functions and responsibilities in the event of a data breach.
- Select an individual with ultimate responsibility for overall implementation of the plan (i.e., the person authorized to make the final decision on difficult questions).
- Identify outside advisors that may need to be contacted in the event of a breach, such as legal, forensic and public relations specialists, as well as regulators and law enforcement authorities.

- Outline each phase of the response plan, from initial response activities (such as reporting the breach) to strategies for notifying affected parties, to breach response review and the remediation process.
- Create hypothetical scenarios to test the plan (i.e., do a practice run) and address any vulnerabilities identified during those simulations.
- Ensure that the plan is reviewed regularly and revised as necessary.

The board should make inquiries to determine whether management has taken each of these steps to the board's satisfaction and has otherwise formulated a comprehensive breach response plan.

10. Non-Digital Information and Physical Devices

What steps does management take to safeguard sensitive non-digital information?

With all the talk about "cyber," it is important to remember that safe and secure storage of non-digital data, as well as proper destruction of documents and devices, is equally essential. To the extent possible, companies should minimize the locations in which sensitive non-digital information is stored and should ensure the safe and secure storage of this data. Some measures they can take include locking office doors and filings cabinets and/or installing card keys on doors. In addition, companies should ensure that documents (as well as disks, DVDs, flash drives and computers) with sensitive information are properly destroyed before disposal (such as by shredding or burning), as dumpster diving is still a common means of stealing data.

Though it will be focused on overseeing cyber risks in the true sense of the term, the board should also make sure to ascertain whether the company's policies and practices adequately protect sensitive non-digital information in the company's possession.

Conclusion

To fulfill its duty of care with respect to overseeing the company's cyber risks – and to be able to demonstrate, in any future litigation, that it has fulfilled this duty – the board must ask thoughtful and strategic questions to understand how management is preventing, detecting and responding to data breaches and incidents and to ensure that it is comfortable that the measures being taken in this regard are sufficient and appropriate. By asking the questions outlined above – and any other questions relevant to the company's facts and circumstances – and by exercising good judgment, directors can successfully oversee the cyber risks facing the company and the company's plan to mitigate and respond to those risks.

Nasdaq Corporate Solutions' Meetx Board Portal is designed to provide public, private, and nonprofit boards and leadership teams with greater governance management, throughout the organization. Built with security in mind, our easy-to-use and efficient software helps companies simplify the sharing of critical information via the web or tablet apps and makes meetings anywhere more productive.

CONTACT INFORMATION:

business.nasdaq.com
corporatesolutions@nasdaq.com

Simpson Thacher & Bartlett LLP is one of the world's leading international law firms, providing coordinated legal advice and transactional capability to clients around the globe.

CONTACT INFORMATION:

Yafit Cohn
(212) 455-3815
yafit.cohn@stblaw.com

Karen Hsu Kelley
(212) 455-2408
kkelley@stblaw.com