In the wake of cyberattacks adversely affecting publicly traded companies, plaintiffs’ attorneys specializing in shareholder lawsuits increasingly are seeking to hold corporate boards responsible. The most common tactic is to bring a derivative lawsuit on behalf of the corporation for alleged wrongdoing by board members causing harm to the corporation. In the case of a cyberattack, the alleged wrongdoing would most likely be breach of fiduciary duty for failure to adequately manage and supervise the company’s data defenses. In the past few years, such lawsuits have been brought against the directors of Target, Home Depot, Wyndham and Heartland Payment Systems, albeit with limited success for plaintiffs. Derivative lawsuits are subject to unique procedural defenses, such as a requirement that a pre-suit “demand” be made on the board of directors unless it can be demonstrated that the directors could not fairly consider the demand.

TAKEAWAYS

charted Public company officers and directors may face legal liability for ignoring cybersecurity risks.

charted The SEC likely will issue new guidance concerning required disclosure in connection with a cybersecurity incident.

charted Directors should also understand and participate in decision-making about other protections such as insurance and SAFETY Act certification.

11.14.17

In the wake of cyberattacks adversely affecting publicly traded companies, plaintiffs’ attorneys specializing in shareholder lawsuits increasingly are seeking to hold corporate boards responsible.

The most common tactic is to bring a derivative lawsuit on behalf of the corporation for alleged wrongdoing by board members causing harm to the corporation. In the case of a cyberattack, the alleged wrongdoing would most likely be breach of fiduciary duty for failure to adequately manage and supervise the company’s data defenses. In the past few years, such lawsuits have been brought against the directors of Target, Home Depot, Wyndham and Heartland Payment Systems, albeit with limited success for plaintiffs. Derivative lawsuits are subject to unique procedural defenses, such as a requirement that a pre-suit “demand” be made on the board of directors unless it can be demonstrated that the directors could not fairly consider the demand.
An egregious failure of the board to direct and oversee the business and affairs of the corporation, if it amounts to conscious disregard of their responsibilities, is deemed a breach of the duty of loyalty. This is significant because, unlike the case of an alleged breach of the duty of care, directors cannot be indemnified by the corporation or exculpated for breach of the duty of loyalty. Also, where a derivative plaintiff can credibly allege such a breach, pre-suit demand on the board is excused. To have a chance of success, a failure of oversight claim will almost always need to allege breach of the duty of loyalty. The usual way in which it is alleged is by pointing to “red flags” that were ignored or addressed inadequately.

An argument can be made that the increasing frequency and severity of cyberattacks is a “red flag” that should draw the attention of corporate directors, even if such an attack has not (yet) struck their company. Principles of good corporate governance suggest that the board should ensure it is adequately informed about the strengths and weaknesses of the company’s cybersecurity program, that it has deliberately considered the actions available with respect to cybersecurity including their pros and cons, and that the board has reached a considered and informed decision that cybersecurity is adequate in light of all the circumstances.

Besides fiduciary duties, public companies may have obligations arising under SEC reporting rules. One such rule requires that contingent liabilities be adequately disclosed and, in some cases, accounting reserves be set up to cover them. Another rule requires that known risks or uncertainties be disclosed if they reasonably may be expected to have a material adverse effect on the company. Board members, especially audit committee members, can be liable under the securities laws if they fail to inform themselves and make reasonable decisions about these types of disclosures. Another rule requires the board to ensure that the company has an adequate system of internal controls sufficient to ensure accurate reporting of financial matters. Failure to comply with securities law obligations potentially can expose directors to liability both as defendants in shareholder lawsuits and in SEC enforcement actions.

Recently, a top official of the SEC told a group of lawyers at a Practising Law Institute Event in New York City that he expected the SEC to refresh its guidance concerning public companies’ duties of disclosure and policies concerning trading by corporate insiders around a data breach. At the same time, the SEC’s enforcement division has signaled increasing willingness to look at whether a company’s public disclosure around a data breach requires additional regulatory scrutiny.

In light of evolving rules and jurisprudence concerning public companies’ duties around a data breach or other cyber incident, the board should work with professional service providers, such as its counsel, to perform a thorough review of the company’s cybersecurity policies, processes, vulnerabilities and protections. Ideally this will be done by the board as a whole, but the task can be delegated to a committee so long as the committee provides a detailed summary of the review to the board as a whole. The directors should do a comprehensive review initially, and then update that review periodically, at least once a year.
The following is a checklist of questions that board members may want to ask. As with any checklist, it is important to listen to the answers and follow up with additional questions when appropriate.

**Personnel and Policy**

It is estimated that over 90 percent of cyberattacks result from human error. Employees must be properly trained and equipped to minimize the probability of such errors.

- Who is the senior-most corporate officer who “owns” cybersecurity? How much time does the officer devote to such issues and how detailed is the officer’s knowledge?
- Who is responsible for day-to-day management of cybersecurity? What are the qualifications of those individuals? How much time do they spend on cybersecurity?
- What are the greatest concerns of the people responsible for managing cybersecurity? What have they done to address those concerns?
- What training has been provided to employees regarding cybersecurity? Have they been trained to spot and report “phishing” attempts and “spoofed” e-mail, and to avoid opening suspicious e-mail attachments? Have they been trained to be skeptical of embedded links to web pages, typing the address into the browser rather than clicking on the link in case of doubt?
- What is the procedure for reporting suspicious occurrences? Who is responsible for investigating and responding? What records are kept, and what reports are made?
- What are the company’s policies with regard to password strength and periodic changes?
- Who has administrator privileges? Is there a single administrator password for all servers and devices or are there multiple passwords? Are personnel with administrator privileges allowed to run their workstations in administrator mode when not required to do so?
- What are the procedures for physical security, such as visitor logs, restricted areas for visitors and logging employees’ use of access keys? Are employees trained to identify and report visitors who are in unauthorized areas?
- What are the procedures for vetting and monitoring outside contractors who have physical access to the workplace, such as janitorial services?
- Does the company have an outside cybersecurity consultant? Has the consultant conducted a recent audit? What did the audit consist of and what were the results? Has the consultant done penetration testing, including use of simulated phishing and other types of cyberattacks?
- What is the company’s policy regarding security of portable media (CDs, DVDs, USB drives, etc.)? Is such media required to be encrypted? Are logs created when employees copy data to portable media? Is there any requirement to make a record of what is on such media, and where it is located? Is there a procedure for wiping or destroying such media when the data is no longer needed?
- Are employees allowed access to company systems using home computers or portable devices? What protections exist to prevent unauthorized access through such connections? Are portable devices
required to have automatic screen lock? Can data on portable devices be remotely wiped in the event of theft or termination of employment?

- Does the company have a cyber breach response plan? What are the details? Does it include creating a detailed record of the events leading up to the breach discovery, notifying appropriate firm IT personnel and external consultants of the breach so they can take necessary steps to stop it, quickly and accurately evaluating the extent and effects of the breach, and developing an internal and external communications plan? Under what circumstances will the Board be notified?

- Who is responsible for ensuring that operating systems and other software are kept up to date with the most recent patches and revisions?

- Do employees have the ability to send data securely when needed, such as through secure e-mail?

**Hardware and Software**

Robust, properly configured hardware and software systems can assist humans in avoiding or identifying and dealing with malicious content.

- Does the company employ technology to prevent employees from accessing malicious websites?

- What protections exist to prevent accessing sensitive data if employee laptops are stolen? Are hard drives encrypted? Can laptops be wiped remotely? Are laptops required to have automatic screen lock after a period of inactivity?

- Does the company have technology to detect and remove or quarantine malware? What are the details? Does the e-mail system scan attachments to detect malware?

- Are computer systems “compartmentalized”—for example, if a single server is breached, is the problem confined to that server or can it readily spread to other servers and throughout the company’s network?

- Are there fail-over systems such that if one server stops working or must be taken out of service another can easily step in to replace it?

- Are backups of data verified for integrity and completeness? Are there redundant copies? Is there a system (hardware, software and procedures) that permits speedy and reliable restoration of data?

**Insurance and SAFETY Act Protection**

Cybersecurity insurance and SAFETY Act certification can mitigate the cost of a cyberattack, if one occurs.

- Does the company have cybersecurity insurance covering both first-party loss (business interruption, restoration or re-creation of data and other remediation costs) and third-party loss to cover any damages to third parties whose data may have been compromised?

- Has the company sought or obtained SAFETY Act certification for its cybersecurity program from the Department of Homeland Security? (Such certification would limit the company’s liability to third parties and would provide an excellent defense to any claim of personal liability on the part of...
A comprehensive cybersecurity program should be part of the company’s enterprise risk management plan, and should be drafted with the assistance of outside counsel and IT professionals. A well-constructed program can protect the company, its officers, directors, shareholders and customers from being the next cyber incident in the headlines.