The cybersecurity scare

There are actions that directors can take to keep themselves within the protection of the business judgment rule.

BY DOUG RAYMOND

Doug Raymond is a partner in the law firm Drinker Biddle & Reath LLP (www.drinkerbiddle.com).

Attentive directors can hardly be blamed for thinking that the sky is falling. Derivative litigation against directors (measured as a percentage of such lawsuits against public companies) has been increasing, ISS and others have been much more active in criticizing—and seeking to unseat—incumbent directors, and there has been a steady stream of new rules and regulations that create ever-increasing burdens on the directors. And on top of this, the board's liability for a "cyber-attack" has become almost a cause célèbre. Clearly, cyber-attack incidents can cause real damage to a company's brand and reputation, and may lead to significant financial losses, as well as dissipate customers' trust and goodwill. The costs of such attacks include not only loss of reputation and the costs of compensating customers, but also the real possibility of regulatory actions and the near certainty of massive litigation.

There have been highly publicized cases over the last few years asserting breach of fiduciary duty and seeking to hold the directors (or their D&O insurers) liable for failing to prevent a significant data breach. However, the plaintiffs in these cases have generally been unable to get around the protection afforded to the board by the business judgment rule.

The business judgment rule is the presumption that the directors, in managing the affairs of the corporation, are acting in good faith in the corporation's best interest. It also presumes that directors when acting are doing so on an informed basis. The rule is designed to protect directors from the risk that they will be liable for making a poor business decision by plaintiff's second-guessing with the benefits of hindsight. As such, the business judgment rule is a presumption that is difficult for plaintiffs to overcome. However, it is possible for a board to be so careless that the business judgment rule no longer affords its protection. Absent a conflict of interest or other breach of the duty of loyalty, this requires the board to have been essentially grossly negligent in discharging its oversight responsibilities.

Thus, under current principles, when a cyber-attack occurs, the board should be protected from liability unless it has utterly failed to implement a reporting or information system covering protection of sensitive data, or consciously failed to monitor or oversee the corporation's defenses against an attack, thus making it impossible to be informed on the issues. If such systems exist and they are reasonably monitored, the directors should be protected even if the defenses fail and a massive cyber-attack occurs. Courts, in dismissing shareholder derivative lawsuits, have offered guidance for boards exercising their oversight responsibilities in connection with cybersecurity. The following are examples of actions that directors can take with respect to data security to keep themselves within the protection of the business judgment rule:

- Discuss at board meetings the types of sensitive information being collected by the company and the security in place to protect such data.
- Empower a board committee, such as the audit committee, to periodically review and evaluate the threat that cyber-attacks may pose to the corporation.
- Authorize the corporation to engage technology consultants or other experts to review the corporation's data security protocols and system defenses.
- Stay informed about the cybersecurity procedures and defenses that the company has in place.
- Push management to ensure that the company has an adequate level of expertise (whether internal or external) to design and implement security protocols, properly assess the risks and system controls, and adequately inform the board about data security matters.
- Require that the company have a plan in place to deal with a data breach, including how the company will identify the scope of the breach, contact any persons affected by the breach, and rapidly repair any damage that may result.
- If a breach does occur, confirm that the plan for dealing with such breaches (see above) is quickly and effectively implemented to manage the liability that may stem from the breach.

Boards may be seeing only the beginning of new challenges created by doing business in such a connected world, and there is little doubt that cyber-attacks will continue if not escalate. However, as has been the case with other corporate challenges in the past, directors can take comfort that, with a reasonable level of diligence, the business judgment rule will protect them from claims that they should be liable for failing to prevent the attack. So long as the board keeps informed about the risks and does not completely ignore preparations to defend against data attacks, these pre-Internet principles of corporate law should keep the sky from falling. ■

The author can be contacted at douglas.raymond@dbr.com. Eric Dante, an associate with Drinker Biddle & Reath, assisted in the preparation of this column.