PROPERTY CASUALTY 360°

How directors and officers can reduce cyber liability exposure

Companies must anticipate the next cyber breach

Jun 27, 2017 | By Vincent J. Vitkowsky, Robert D. Laurie

Although no cyber liability measures are bullet-proof, certain decisive steps can go a long way toward affording a strong defense against shareholder derivative lawsuits. (Photo: iStock)

As high-profile data breaches have become commonplace, class actions and individual lawsuits are frequently commenced by customers and employees whose personal data has been exposed.

Claims against the corporations themselves have had mixed success in pleading causes of action that survive past motions to dismiss. Plaintiffs have also struggled to demonstrate concrete, particularized injuries sufficient to confer standing, *i.e.*, status to sue.

Directors and officers (D&O) have consistently fared well in shareholder derivative actions alleging that they have failed to implement proper cybersecurity measures that would have

prevented the breach. Consider that three recent prominent cases, against Home Depot, Target, and Wyndham Hotels, have been dismissed.

5 essentials of a Cyber liability insurance policy

Privacy liability covers far more than just a data breach.

The basic legal analytical framework favors directors and officers. With some variations across states, the business judgment rule protects them from personal liability by setting a strong presumption that they have acted on an informed and reasonable basis, in good faith, and in the belief that they were acting in the best interests of the company.

Favorable precedent

The most recent decision came in December 2016, in the case of *In Re Home Depot, Inc. Shareholder Derivative Litigation*, 2016 WL 6995676 (N.D. Ga. Nov. 30, 2016). The case arose from a 2014 data breach that revealed the credit card numbers of 56 million customers. Plaintiffs alleged that Home Depot's directors and officers had breached their duty of loyalty by failing to institute sufficient internal cybersecurity controls, and by disbanding the Board's "Infrastructure Committee," which was responsible for oversight of cybersecurity risks. They also alleged waste of corporate assets. Finally, they alleged violations of Section 14(a) of the Securities Exchange Act.

The court applied Delaware law, which requires that before a suit can be commenced, the plaintiffs must make a formal demand on the Board to have the company commence an action based upon their allegations. If they do not make that demand, plaintiffs must make particularized allegations creating a reasonable doubt that the Board could have exercised its independent and disinterested business judgment in response to the demand. This would ultimately require a showing that the conduct complained of is so egregious on its face that Board's action or inaction cannot meet the business judgment test, so that the directors would have been subject to a substantial likelihood of liability. Plaintiffs would thus establish that a demand on the Board would have been futile.

In dismissing the complaint, the court addressed each of the three claims. On the breach of loyalty claims, the court concluded that the Board had not consciously failed to take adequate measures. Although it had transferred oversight authority to the Audit Committee, that Committee regularly received cybersecurity reports and kept the Board informed. The Board approved a plan to correct known cybersecurity weaknesses. The court held that even though in hindsight, the Board may have been too slow to implement better security, Board decision-making must be "reasonable not perfect."

Shareholders continue to bring lawsuits against directors and officers in the face of cybersecurity breaches. (Photo: Shutterstock)

Addressing the corporate waste claim, the court found that the Board's decision to implement cybersecurity measures slowly — even if it ultimately proved to be too slowly — was within the discretion of the Board and protected by the business judgment rule.

Related: **Not all data breaches are created equal**

The alleged securities violations related to statements in the 2014 and 2015 Proxy Statements. The court ruled that plaintiffs had failed to identify specific misleading statements, and failed to show causation because the breach was already underway at the time of the 2014 Proxy Statement.

Insurance mitigated cost of breach

Then, in July 2016, the case against Target's directors and officers was also dismissed. *Davis v. Steinhafel*, No. 14-cv-203 (D. Minn. July 7, 2016). That dismissal followed a different route. Target was hit with a data breach in late 2013 that affected up to 110 million customers. Shareholders brought various actions alleging that the company "failed to take reasonable steps to maintain its customers' personal and financial information," and also alleging that the company actively attempted to conceal the extent of the breach and failed to provide prompt and accurate information about the breach.

Target is a Minnesota company, and Minnesota law requires the formation of a Special Litigation Committee (SLC) to evaluate a shareholder demand. Target appointed an SLC consisting of a former Minnesota Supreme Court Justice and a University of Minnesota Law

Professor. The SLC conducted an extensive investigation, with the assistance of independent counsel, over a 21-month period, and produced a 91-page report. It concluded that it would not be in Target's best interests to pursue the claims.

Under Minnesota law, the court's review of such a report is limited to whether the SLC was disinterested and independent, and conducted a good faith investigation. Under these circumstances, the shareholder plaintiffs did not challenge the SLC report, and the court dismissed the actions. Among the factors that were important to the SLC in reaching its conclusion were the following. There were pre-breach policies and procedures that incorporated technical, administrative, and physical controls for data security. There were pre-breach vendor security procedures. There was employee training on data security. And the cost of breach was mitigated by the existence of network security insurance.

Implemented additional security measures

Similarly, in late 2014, in *Palkon v. Holmes*, 2014 WL 5341880 (D.N.J. Oct. 20, 2014), claims against the Board of Wyndham Hotels were dismissed. Over the course of three breaches between 2008 and 2010, hackers obtained more than 600,000 payment card numbers and engaged in more than 10 million in fraudulent transactions. From the time of the first breach, the Board met to discuss the breaches and security measures 14 times, and its Audit Committee met to do the same at least 16 times. Between the second and third breaches, Wyndham had begun to implement additional security measures.

Related: Data obstacles hamper cyber insurance growth

Like *Home Depot*, this case was decided under Delaware law. Upon being presented with an initial shareholder demand, the Audit Committee hired the law firm of Kirkland & Ellis, one of Wyndham's usual outside general counsel, to investigate. The firm found the demand was not well founded, and the Board voted not to pursue a lawsuit. A subsequent shareholder made a similar demand, which the Board again rejected. The second shareholder commenced an action alleging breach of fiduciary duties, corporate waste, and unjust enrichment. The court dismissed that complaint on the grounds that the Board's refusal to commence a lawsuit itself was a made in good faith, after a reasonable investigation, in the exercise of business judgment. The court rejected claims that both Kirkland & Ellis and Wyndham's in-house general counsel had conflicts of interest.

Pending actions

Despite these decisions, it would be premature to conclude that no viable claims can exist, because a fact pattern may well emerge that would allow plaintiffs to proceed beyond a motion to dismiss. And shareholders continue to bring actions against directors. Among the actions currently pending are those against The Wendy's Company and Yahoo! Inc. (now part of Oath, a Verizon company).

Directors can reduce or minimize their potential liability by taking reasonable measures appropriately designed to meet the cybersecurity threats faced by their companies. (Photo: iStock)

Reducing potential liability

Although the plaintiff's bar will continue to commence new actions, directors can reduce or minimize their potential liability by taking reasonable measures appropriately designed to meet the cybersecurity threats faced by their companies.

Most generally, companies need to have a specifically-tailored cybersecurity program. In crafting the program, companies should seek to comply with all relevant statutory or regulatory requirements and guidance. Although these will vary by industry and state, some key requirements and guidance with widespread applicability include the following.

No 1: State pre-breach security measure laws

Certain states have general laws requiring pre-breach security measures, generally requiring only that they be "reasonable." The California Attorney General has taken it to a greater level of specificity. Its February 2016 Data Breach Report states that failure to implement the Critical Security Controls of the Center for Internet Security constitutes a lack of reasonable security.

No. 2: National Institute of Standards and Technology ("NIST") Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity

This is an ostensibly voluntary risk-based compilation of guidelines intended for critical infrastructure industries. It compiles various core practices within the context of five functions. They are:

- Identify,
- Protect,
- Detect,
- Respond, and
- Recover.

These are broken down further into subcategories that describe "informative references" to particular activities, which are meant to illustrate methods to achieve related outcomes. Boards in many industries are inclined to treat compliance with the NIST standards as near-compulsory.

No. 3: New York Department of Financial Services ("NYDFS")

Banks, insurance companies, and other companies regulated by the NYDFS are subject to its, "*Cybersecurity Requirements for Financial Services Companies."* These went into effect on March 1, 2017, and established various compliance deadlines, ranging from 180 days to two years. In addition to various granular measures, its major components include requirements that covered entities do the following:

- establish a cybersecurity program and documentation;
- adopt a written cybersecurity policy and incident response plan;
- designate a Chief Information Security Officer responsible for the program and policy;
- adopt a third-party service provider security policy to secure information systems and nonpublic information accessible to or held by third-parties; and
- submit an annual certification of compliance by the Chairman of the Board or a Senior Officer.

Reducing potential liability

In general, to reduce or minimize their own liability, directors and officers should implement the following measures:

- develop comprehensive enterprise Cybersecurity Policies and Procedures, which need to be continually updated;
- ensure compliance with all relevant regulatory sources;
- the Board should meet frequently — at least quarterly — to review cybersecurity issues;
- develop specific cybersecurity programs, with established metrics and benchmarks; and
- develop procedures for reviewing the cybersecurity of third parties with which the company interacts.

In addition, directors and officers should consider the following measures:

- obtaining cyber insurance;
- establishing a Cybersecurity Subcommittee to the Audit Committee, which could include at least one technical expert, to make recommendations to the Board on its cyber responsibilities;
- the Board could pre-approve cybersecurity software, hardware, and consultants;
- the Board could pre-approve retention and oversee any security firm and data breach response professionals, including attorneys, engaged by the company;
- the Board could retain independent security experts to assist the Audit Committee and any Cybersecurity Subcommittee;
- appoint a director with cybersecurity expertise.

These measures are not bullet-proof. No measures can be. But they will go a long way toward affording a strong defense against shareholder derivative lawsuits.

Vince Vitkowsky is a partner at the law firm Seiger Gfeller Laurie LLP. Robert D. Laurie is a founding partner of the firm. They serve insurance and reinsurance companies in litigation, counselling, and product development in many lines of business, including cyber, CGL, E&O, AND D&O insurance. For more information, visit www.sgllawgroup.com.

http://www.propertycasualty360.com/2017/06/27/how-directors-and-officers-can-reduce-cyber-liabil?ref=hp-news&slreturn=1499737288&page_all=1