Are Directors Accountable After a Cyber Breach?

By Jennifer Williams-Alvarez November 12, 2018 · 0 Comments · Post Comment

When a company suffers a cyber breach, the associated costs can easily soar into the hundreds of millions of dollars. Equally damaging for a company is the potential hit to its reputation. Meanwhile, directors are increasingly a focal point for regulators in the management of cyber risk.

Up to now, it hasn't been commonplace for directors to be held accountable after a breach, whether in terms of losing their seat on the board or facing liability in court. But the current landscape may be due for a change, sources suggest.

For one, regulators and lawmakers have increasingly determined that cyber-risk oversight responsibilities rest on the shoulders of the board, points out **Craig Newman**, partner at law firm **Patterson Belknap Webb & Tyler** and chair of the privacy and data security group. "There is clearly a regulatory trend toward placing more accountability on corporate boards when it comes to oversight of cyber-security risks," he says. "There are only a handful of regulations and laws that create either dotted lines or straight-line responsibility directly to boards, but I think we're seeing a gradual shift."

Whether that in any way is an indicator of increased accountability on other fronts, either in the form of liability in court or the loss of board seats, Newman says, "It's too early to tell."

If directors are paying attention and effectively overseeing the company when it comes to cyber security, they will likely continue to fare well when it comes to liability, says **John Reed Stark**, president of **John Reed Stark Consulting** and a former chief of the **Securities and Exchange Commission**'s Office of Internet Enforcement. But if they fail to establish policies and ensure they are informed and asking the right questions, Stark says he believes directors are increasingly at risk of being held liable. And currently, these are steps he does not believe many boards are taking.

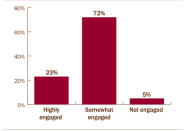
That's a reality that likely has to change, says Stark. "I do think there's a growing expectation that boards are focusing [on cyber]," he says. "Because a cyber attack can be deadly to a firm, to its operations, to its financial status, to its reputation, to its culture."

If that's not motivation enough to act, the fact that plaintiff's attorneys continue to look for ways to hold directors liable in court might be, Stark notes. "The one thing that pushes boards more than anything else is the potential for personal liability," he says.

The Director's 'Armor'

The steady drumbeat of headlines and regulatory filings related to cyber incidents has shown the costs of a breach, in terms of both the bottom line and a company's reputation. **Altaba** (formerly Yahoo), for one, revealed in a September regulatory filing that just the latest estimated net amount spent in relation to three cyber-related litigation matters was roughly $47 million. And Google faced backlash, and at least two shareholder suits, following a report by *The Wall Street Journal* that in March, the company discovered a software glitch that exposed user data on Google+, its social network, between 2015 and the time of discovery. Google then opted not to disclose the issues, according to the *WSJ*.

It is no surprise then that cyber issues remain a top concern for boards. Indeed, 27% of CEOs and board directors said cyber incidents or events pose the greatest threat to their organizations' growth prospects, according to a **Deloitte** survey of 400 CEOs and board members at U.S. companies with at least $1 billion in annual revenue. Forty-two percent of board members further responded in the 2018 CEO and board risk survey that security risks, including both physical and cyber breaches, pose the greatest reputational threat in the following 12 months. But while cyber ranks as a top concern, only 23% of director respondents identified as "highly engaged" when it comes to cyber risk, the numbers show.



Source: Deloitte's 2018 CEO and board risk survey

The incentive for boards to become more involved on cyber issues should stem from their role in driving performance, says **Gunjan Sinha**, executive chairman at governance, risk and compliance consulting firm **MetricStream**. "There is ample evidence that this is very closely tied to performance, and that means that [directors] have to use their business judgment and they have fiduciary duties," he says. "The boards have to demonstrate competency and objectivity on these matters," especially if they are questioned by shareholders in court, he says.

But despite the frequency with which companies are breached, boards have yet to become the target of widespread scrutiny, aside from egregious cases. For instance, following the breach at **Equifax** that exposed the data of more than 147 million U.S. consumers, proxy advisory firms advised against electing some of the directors.

Institutional Shareholder Services, for one, recommended a vote against five directors who were members of the company's audit and technology committees at the time of the breach. "Evidence suggests that the board was aware of the vulnerability, albeit perhaps too willing to believe former CEO **[Richard] Smith**'s assurances that the company had 'world-class state-of-the-art technology,'" ISS said. "The board featured a technology committee — something that many of its peers still lack — although the effectiveness of that committee was arguably undermined by the inclusion of directors who lacked direct technology expertise."

And yet while some directors, including Chairman **Mark Feldler**, received a significant number of votes against their appointment to the board, shareholders ultimately voted to elect the entire slate of 10 directors, as *Agenda* reported.

Directors may also be swept up in litigation related to a breach. Not too long ago, these cases would more than likely be dismissed, as was the case in suits related to breaches at **Target** and **Wyndham Worldwide**. Following the high-profile data breach at **Home Depot**, defendants were similarly granted a dismissal in response to a consolidated derivative action by Judge **Thomas Thrash** of the **U.S. District Court for the Northern District of Georgia** in Atlanta. The plaintiffs then appealed, and a settlement was reached stipulating that the company would pay up to $1.125 million of plaintiffs' attorneys fees.

In fact, other cases have resulted in settlements as opposed to dismissals. Such was the result after **Wendy's Company** directors were the targets of a shareholder derivative complaint in late 2016, following a data breach, alleging that directors and executives "breached their duties of loyalty, care and good faith" in failing to exercise their oversight duties and implement effective internal controls and procedures. This spring, the company came to a settlement with the plaintiffs, which included agreements to implement remedial measures and pay nearly $1 million in attorneys' fees.

Shareholders and their attorneys continue to pursue these claims. Equifax directors, for instance, were hit with a handful of derivative suits early this year, which have since been consolidated in the Northern District of Georgia in Atlanta. "Equifax's officers and directors consciously failed to act in the face of a known duty to protect the confidential data entrusted to the Company and merely paid lip service to maintaining data security," the complaint reads, adding that these failures resulted in the "largest and most costly data breach … in corporate history." Equifax has yet to respond to the complaint, according to the case docket, and the company declined to comment for this article, noting that, as a policy, Equifax does not comment on litigation.

Though some cases have resulted in settlements, sources say they have not seen directors held liable yet. "I'm not privy to a single case where the responsibility has been placed that high in the organization," says Patterson Belknap's Newman. "Board members have some rightful armor when it comes to their role," he explains.

But the risk is there that this protection will be lost if boards fail to implement appropriate governance and policies to ensure directors receive candid and independent information about what's going on within the company as it applies to cyber risks and protections, Stark warns.

At some point, directors will be held responsible in court, and will also face challenges to their positions on the board, says **Kathy Misunas**, director and member of the cyber committee at Wi-Fi network provider **Boingo Wireless**. "Eventually, those types of, if you will, punishments are going to occur," she says.

In addition, beyond the courts, the SEC, in particular, is putting direct responsibility on directors, says Misunas, who is also chair of the CyberTech committee at **Tech Data Corporation**, an end-to-end distributor of technology products. In February of this year, the commission updated its guidance on cyber-security disclosures, explicitly calling for more disclosure about the board's role in managing cyber risk. "The SEC guidance documents are pretty clear about responsibilities of the board, and just because they have not taken action before does not mean they won't in the future," she says.

This focus has already reached, and will continue to reach, beyond the SEC, according to Sinha. He believes that "sooner rather than later" boards will be faced with a cyber-focused law not unlike the one signed into law in September in California, which requires companies based there to have at least one woman on the board by the end of 2019. Instead of focusing on gender diversity, the law would focus on whether a board's composition is adequate when it comes to cyber comprehension and experience, explains Sinha.

"Companies need to defend and understand why their boards are composed the way they are" as it relates to cyber, he says.

Purchase a Reprint of This Story

Tags: Regulation , Legislation , Legal

Comment or Feedback

Keep Me Posted · Comments Moderation · User Preferences

Name Alias *
Company
Anonymous
Comment: *
Post as a Comment Send Feedback to Editor

* Required
Agenda will send a confirmation email to your registered email address.
Post Comment

Topics

All Topics

Compensation · Legal & Regulatory · Nomination & Governance · Audit & Risk Management

Compensation - Total Comp/Plan Design
- Will 'Unique' LTIP Metric Make Microsoft a Trendsetter?
- Pepsi-John's Reels Up Severance Protections Ahead of Expected Sale
- Gig Workers Could Be Paid in Stock

Compensation - Disclosure
- Will 'Unique' LTIP Metric Make Microsoft a Trendsetter?
- 'Massive Gotcha' From IRS on CEO Comp

Compensation - Perks & Agreements
- A Perk at Executives' Sky-High Aircraft Perks
- SEC's Settlement With Dow Turns Spotlight to Perks

Compensation - Director Pay
- CEO Pay Rises by Nearly 10%
- Potential $300 Million Jackpot for GE's New CEO
- Campbell Cuts Bonus Awards Amid Activist Fight

Most Popular

Last 3 Issues

Read · Emailed · Saved · Commented

1 Judge Removes CEO, Director From Company
2 Key Board Leader Skills Not Found on CV
3 Should Ghost Revenue Scare Comp Committees?
4 ISS Proposes New Policy on All-Male Boards
5 Nom-Gov Sees Mounting Reelection Concerns