The Cyber Ecosystem: Evolving Tech And Risk Governance

Law360, New York (February 23, 2017, 11:45 AM EST) --

Boards of directors have consistently named cybersecurity as one of the top issues that they believe requires additional board focus. This is perhaps unsurprising given the fast pace of technological developments and the volatility of the cyberthreat environment. Whether it is Mirai and Leet-based botnets, the military's use of smart phones and tablets to order fire missions, or the latest leak of consumer personally identifiable information (PII), cyber issues regularly top news headlines.

The volume and velocity of cyberattacks is increasing, and so is our interconnectedness, fueled by growing use of internet of things (IoT) devices. In a conversation with Dr. Shue-Jane Thompson, partner for the IBM Cyber and Biometrics Service Line, Thompson noted that in our highly interconnected reality, "cyber physical and logical boundaries are both diminishing." Hence, companies must find ways to adeptly and nimbly address cyberrisks in order to navigate a myriad of business and legal concerns.

The Risks and Consequences Are Real

As part of setting an enterprise's overall risk appetite, the board of directors should determine a specific cyberrisk appetite, too. This is not an issue to be addressed once and be done with. Boards need to regularly and recurrently discuss cyberrisk — a point recently emphasized by three federal banking regulatory agencies in an October 2016 advance notice of proposed rulemaking on a set of potential enhanced cybersecurity risk-management and resilience standards. Boards may choose to task a committee (such as the audit or risk committee) with responsibility for cybersecurity, but cyber issues should not be siloed because effective cyberrisk management requires cross-functional collaboration and consideration of a range of business assets embedded in the workforce, data, technology and facilities. After all, hackers seek not only PII (e.g., Social Security numbers), but intellectual property, insider investment information and confidential communications.

In the extreme scenario, a court could conclude that a board's failure to address cyberrisk constituted a breach of fiduciary duties. By way of background, under state law directors owe fiduciary duties to the corporation and its stockholders, and Delaware corporate law is generally considered the most influential of state law corporate jurisprudence. Delaware corporate law, however, sets a high bar for demonstrating a breach of the "duty of oversight" (a subset of the duty of loyalty), under which the board's risk-management function falls. The core inquiry in any Caremark duty of oversight claim is whether it would be reasonable to infer that the board of directors "intentionally disregarded their fiduciary duties in bad faith," as the Delaware Chancery Court recently reiterated in Reiter v. Fairbank CA No. 11693-CB (Del. Ch. Oct. 18, 2016). Nonetheless, given the other potentially adverse effects of cyberbreaches, this high bar for a breach of fiduciary duty claim shouldn't dissuade boards from striving to proactively and effectively address cyberrisks.

First, hackers who target proprietary intellectual property can undercut a company's competitive advantage. That's arguably what happened to U.S. Steel Corp. In a 2010 attack, hackers stole

intellectual property relating to the production of cutting-edge, high-strength steel. While a federal grand jury in Pennsylvania eventually indicted five members of the Chinese military's cyberespionage division for stealing trade secrets from certain companies, including U.S. Steel, this indictment did nothing to recompense U.S. Steel. So U.S. Steel decided to take an innovative approach, appealing to the U.S. International Trade Commission and bringing broad claims seeking to block imports of Chinese steel products. An administrative law judge initially dismissed the antitrust component of U.S. Steel's claims, but the commission decided to review that decision and the case is now set for a March 2017 hearing.

Second, cyberbreaches often mean resignations and turnover in senior management, which generally isn't good for business. The reputational loss and diminished goodwill triggered by cybersecurity breaches can result in CEO resignations — think Target and the Democratic National Committee. Additionally, hacks reveal emails. These second-by-second written records may show senior management to have engaged in embarrassing personal behavior, improper "joking," and even discriminatory and prohibited conduct. These revelations can trigger management resignations. For example, Avid Life Media Inc.'s chief executive officer Noel Biderman resigned in the wake of a 2015 hack of Avid Life's subsidiary, Ashley Madison — an online dating service marketed to people who are married or in committed relationships. Biderman stepped down just days after hackers leaked private emails from Biderman's corporate account suggesting that he had engaged in a three-year affair with an escort, despite public statements that he had never cheated on his wife.

Third, security breaches mean increased exposure to consumer litigation and securities fraud litigation — and these legal risks may well increase in coming years. In order for a class action to prevail in consumer litigation, plaintiffs must be able to demonstrate harm. Harm is generally shown by a drop in stock prices. In most instances where companies announce breaches, those breaches involved the disclosure of customer PII, rather than the theft of intellectual property or management-team emails. So while breach announcements have not generally been accompanied by persistent and economically significant stock price drops (see "Cyber-Risk Disclosure: Who Cares?" in which researchers Gilles Hilary, Benjamin Segal and May Zhang perform quantitative analysis of breaches affecting U.S.-listed firms), this says little about market reaction to more robust breach announcements. Regulators such as the U.S. Securities and Exchange Commission see cybersecurity as a high-priority item. To the extent companies begin to make more meaningful, robust and timely disclosures of breaches — including hacks of intellectual property, confidential business and financial information, and management emails — more significant market reaction is likely. Consequently, future class action litigation may see a higher success rate.

The question of required disclosures impacts securities fraud litigation, too. The SEC's rules (2011) on disclosure require only that publicly traded companies report hacking incidents that could have a "material adverse effect on the business." Disclosures by companies have tended to be broadly worded and focused mostly on PII. While the SEC has investigated companies and issued comment letters, it has yet to bring a regulatory enforcement action against a company specifically for the failure to disclose a cyberincident. (The Morgan Stanley Smith Barney LLC 2016 settlement, which included payment of a $1 million penalty, for example, was related to a failure to protect customer information, some of which was hacked, but not a failure to

disclose.) Given the current disclosure requirements, it has been difficult for litigants to demonstrate harm stemming from a company's false statement or failure to disclose a breach. In sum, stockholders, the market and even companies themselves, may not be fully aware of the impact that cyberattacks are having on corporate profitability.

Strategies for Resilience

While "there's no finish line in cybersecurity," according to Harry Wingo, professor at the National Defense University, companies can manage their cyberrisk exposure by developing robust policies and procedures. Such policies and procedures can increase resilience to cyberattacks and decrease vulnerabilities, thereby lowering overall cyberrisk and helping ensure a healthy bottom line.

As an initial step, companies need to develop, or consider enhancing, their enterprise cyberpolicies and procedures. In developing and implementing cyberplans, companies should consider leveraging a cross-functional approach that accounts for all aspects of an enterprise's assets, including its workforce, data, technology and facilities. The federal government's 2016 "Cybersecurity Strategy and Implementation Plan" (CSIP) sets forth five priorities, which companies can use to benchmark key components of their own cyberpolicies and procedures: (1) identify and protect "crown jewels" (i.e., high-value information and assets); (2) timely detect and rapidly respond to cyberincidents; (3) rapidly recover from cyberincidents and quickly incorporate any lessons learned; (4) recruit and retain high-quality cybertalent; and (5) efficiently and effectively acquire and deploy existing and emerging technology.

Cybervulnerabilities and attacks know no boundaries — whether geographic, political or economic. Hence, companies may wish to develop information-sharing arrangements with other industry players, or even public-private partnerships. With regard to the latter option in particular, companies should carefully consider how their objectives and those of the government are aligned, and weigh the potential benefits and costs of a partnership. The Commission on Enhancing National Cybersecurity has emphasized the importance of bolstering partnerships between all levels of government and the private sector "in developing, promoting and using cybersecurity technology, policies and best practices," as discussed in the 2016 "Report on Securing and Growing the Digital Economy." Whether private information-sharing arrangements or public-private partnerships, such collaborative efforts domestically may be a harbinger to further arrangements or partnerships internationally, thereby more robustly addressing the global nature of the cyber ecosystem.

Finally, companies should strive to stay abreast of industry best practices in developing their cyberplans. To this end, companies may wish to consider security assessments, monitoring and penetration testing. Comprehensive and multidisciplinary threat and vulnerability assessments can identify and address weaknesses in an enterprise's technology systems and policies, thereby helping the enterprise to better mitigate risk. Ongoing monitoring of systems and devices benefits an enterprise by quickly alerting it to potential threats to its traditional system infrastructures, as well as to the mobile, IoT and other traditionally unconnected devices in use by its employees. This latter grouping of unconnected devices is of key importance because it provides an ingress for threat actors into an enterprise's system infrastructures. Lastly,

penetration testing facilitates an enterprise's understanding of the weaknesses in its security systems, thereby allowing the enterprise to develop more robust security mechanisms. Importantly, penetration techniques can be applied not only to a network perimeter, but also to an enterprise's traditionally unconnected devices and application presence.

Conclusion

In our ever developing cyber ecosystem, it seems that with each new day, we awaken to the next new frontier of cyberthreat. There is no final frontier. For companies, therefore, the question of cybersecurity becomes a matter which requires ongoing agility and focus, and the development of robust policies and procedures. Moreover, while the latest strain of cyberattack will trigger certain immediate consequences for a company — perhaps the loss of cutting-edge trade secrets — other business and legal repercussions may develop over time in ways both expected and unforeseeable today.

—By Sonja S. Carlson, Sheppard Mullin Richter & Hampton LLP and Mingu Lee, Samsung SDS America