NACD PROGRAM

February 16, 2016

Cybersecurity 2.0: What Can Your Board Do Besides Lose Sleep?

On February 16, the Chapter hosted a panel of cybersecurity experts who gave practical tips to board members on this important boardroom topic. Dave Weinstein, Chief Technology Officer for the State of New Jersey, was joined on the panel by Jim Ambrosini, head of Cohn Reznick's cybersecurity practice, and Ken Rashbaum, partner in the law firm Barton LLP. Anita Allen, Chapter Treasurer and President-Elect, moderated.

Mr. Weinstein framed the issue as an important risk management issue for the Board, but it is an issue on which the State can be helpful to New Jersey companies. The State's web site, cyber.nj.gov, contains a wealth of helpful information, including threats on which the State has "actionable intelligence." It also serves as a clearinghouse of technical information that should facilitate a risk based approach. Currently, hackers appear to be looking for targets of opportunity whose cyber hygiene shows vulnerability. Barriers to hacking are increasingly getting lower and attack vectors are increasing, such as through the growing emphasis on the 'internet of things." Boards must engage in a balancing act, weighing the need for security against operational efficiency.

Mr. Rashbaum emphasized that the trend in the law is to hold Boards accountable for data breaches and that the application of the business judgment rule in this area is eroding since the risk is being looked at as a compliance risk, rather than a business risk. Courts are looking at a "head in the sand" approach negatively, as an approach that is not being taken in good faith. Although the law doesn't require Boards to plug all risks, "reasonable" steps must be taken to protect cyber information and the cases are replete with detailed roadmaps that cover do's and don'ts, such as cases involving Wyndham and Home Depot. Reasonable steps would include bringing in outside counsel to investigate a data breach and documentation of all steps the Board is taking in response. He further cautioned Board members to double check the company's D&O policy, since some insurers have begun to exclude cyber risk from coverage. He also reminded the audience that emails between Board members are discoverable and hence in the case of a data breach should be drafted with special caution.

Mr. Ambrosini reminded Board members that they have a role that is not directly engaged in cyber security, but rather an oversight role that should emphasize identifying holes in the company's security and plugging them first. Too many companies erroneously assume they have adequate protection if they pass "penetration tests" seeking to simulate an actual break in. Areas of Board focus should include risks from third parties, staff training and identification of the company's "crown jewels," the theft of which could be catastrophic. Encryption of information is becoming more widespread and does make hackers seek vulnerabilties elsewhere, but should not be seen as a "safe harbor" since administrator credentials can be stolen. It is important to build in layers of security rather than to try to erect a fence around sensitive information.

Questions from the audience brought out other points from the panel. More frequently, a company's cybersecurity protection is increasingly becoming the subject of the annual audit. Although having a cybersecurity expert on the Board is helpful, and the SEC may be considering whether to require disclosure in this regard, it is most important that all Boards generally have sound base knowledge and sufficient training in the area. Smaller organizations should be especially cautious, since hackers consider them "low hanging fruit." Board members should be in contact directly with the company's personnel responsible for security, and the panel cautioned against developing a false sense of security by interacting solely with the CIO. Another danger area is "spoofing," where the organization is used to hack others. Manufacturers dealing with offshore supply chains need also to be wary about what is going on overseas, not an easy task. There are about 30 to 40 writers of D&O cyber insurance, but a standard policy has not yet evolved, so there are many differences. Management's answers given on the D&O application need to be scrutinized with care, since a "wrong" answer can lead the carrier to cancel the policy exactly when it is needed the most.

The NACD has developed specific cybersecurity resources to help directors handle the risk. Specifically, NACD has recently published a Cyber Risk Oversight Handbook for Directors and has established an online Cyber Risk Oversight Program course that leads to the award of a Certificate of Cybersecurity Oversight. Additionally, the NACD conducts an annual Cyber Summit to be held this year on June 21 in Chicago.