MARCH 10, 2016
CHAPTER EVENT SUMMARY

Cyber Security: Tales from the Breach

Moderator: **Cam Kerry – Senior Counsel, Sidley Austin; former General Counsel for the US Department of Commerce**

Panelists: **Kevin Elliot – Senior VP, Hill Knowlton Strategies, Director of Risk Crisis Communication**

Shawn Henry – President and CSO, Crowdstrike Services; retired Executive Assistant Director of the FBI

Frank Modruson – retired CIO, Accenture; director, Zebra Technologies, Forsyth, Inc.

Kerry set up the afternoon's program by noting the changes that have taken place in the area of cyber security over the past two years. Concerns have moved beyond the credit card and email breaches that occurred at companies like Target, Home Depot and Sony in 2014 to more all-encompassing risks regarding system shut downs, encryption ransom and the loss or theft of key operating data. In 2014, 59% of directors indicated they were spending increased time and effort on cyber security issues with that number rising to 69% just one year later; one-third of directors devote at least a portion of a board meeting each quarter to the topic of cyber security, with close to 90% having discussed the issue in at least one board meeting during the past 12 months. Kerry and his panelists spent the remainder of the presentation discussing the best use of board time in addressing cyber security concerns and prevention.

1. Cyber security is a clear business risk and therefore a board responsibility, according to Henry. Directors should ignore claims from executives who declare their companies are not targets of cyber breaches because "we have nothing of value." Any corporate asset – and every company has information, data or intellectual property that are proprietary and key to running their business – is at risk from nation states or international competitors looking for a competitive edge and/or organized crime entities interested in collecting ransoms for encrypted data. In the most terrifying scenarios, medical devices could be reprogrammed to hurt the people they're designed to help, and power and communication grids could be compromised.

2. Elliot declared that every company will suffer – and survive – a cyber breach at some point. Moreover, he believes that companies will be judged on their response, not the fact that the incident actually occurred. Board members can be effective by breaking down internal constraints that operating management cannot, particularly in the areas of corporate training and preparedness.

3. Cyber security preparedness involves people and processes as well as technology, and breaches can come in any one of these three areas. Modruson recommends that board members make sure companies have strong preparedness training in addition to effective firewalls, and these protection measures should cover vendors as well. In terms of processes, the CSO management structure is very important, and Modruson believes the CSO should report to someone other than the CIO to ensure independence between the

"watchers" and the "groups being watched;" a "healthy tension" provides more candor and better preparedness. Elliot recommended a direct reporting relationship between the CSO and the CEO. Lastly, the CSO should be part of due diligence procedures during M&A activity, including determining the value of any intellectual property that may be part of the transaction. Henry suggested that board members find out if potential acquisition targets have incurred security breaches in the past.

4. Only 4% of board members describe themselves as "tech savvy," so Modruson recommended that directors educate themselves about cyber security issues in a number of different ways. Begin by asking the CIO and CSO about the type of cyber security the company uses and ask for updates on implementation status. Ask to see a summary of the company's incident logs; if the company has no incidents listed, it is much more likely they are not detecting them than that none are taking place. Moving beyond internal research, Modruson noted that there are a number of websites offering industry-specific recommendations for preparedness and prevention, and Henry recommended that boards consult outside experts to monitor the company's plans and preparedness.

5. In terms of board communication, the panel agreed that a monthly briefing cycle was probably the optimal time frame for updates, although some companies do so bi-weekly.

6. Preparedness plans must include "white hat" attacks or penetration testing. The panelists all agreed that this type of testing should take place at least annually with results reported to the board on a timely basis. Potential breaches tied to people and/or processes should be dealt with through additional training and actions against repeat offenders as necessary.

7. In the event that a cyber breach does occur, audience members asked the panelists what they, as directors, should expect from the CEO and management. Elliot noted that CEO's should communicate quickly to the board that the company is prepared; the CEO should be able to state clearly, "We know how the public will respond. We have a well-crafted plan with clarity about internal roles, and we tested the plan three months ago. We know that we must behave like the responsible company we are. We are going to survive, and we will be stronger." Henry urged directors to make sure early on that the company "has stopped the bleeding" and is not still losing data. Modruson advised directors to realize that the facts will change in the initial days as management collects information on the extent of the breach and the damage it may have caused. From a public relations standpoint, Elliot noted that law enforcement concerns may initially limit what the company can say publicly, but the company should have already identified key stakeholders and should have the capacity in place to communicate with employees, clients and vendors when appropriate. In essence, the board's largest role in this process is actually before an incident takes place, making certain that management is properly engaged and prepared.

8. The panel discussed the role of the government in helping companies avoid cyber security breaches. Henry believes there is a misconception that the federal government plays a larger oversight/protection role than it actually does; the US government is not protecting computer systems on a day-to-day basis. It will use "tools" such as diplomacy and economic sanctions to prevent breaches or deal with issues after they occur, but government agencies will not, for example, react "in kind." Audience members continued the dialogue, asking question about what they, as business leaders, could do to encourage the government to deploy resources, as well as the legal responsibilities of firms when customer data or money is stolen.