Cybersecurity: What Directors Need to Know

Nora Denzel, Ericsson director and board member of the NACD Northern California Chapter, moderated an active panel and audience discussion on cybersecurity in the boardroom, hosted by the NACD Florida Chapter. The panel consisted of leading chief information security officers (CISOs) from companies such as Lennar, Royal Caribbean, and AutoNation.

Cybersecurity Focus in 2018: What the CISOs Had to Say

Juan Gomez-Sanchez, CISO of Lennar Corporation, kicked off the discussion with what he believes will be a trend in 2018: shifting cybersecurity focus from defensive capabilities to offensive capabilities. Expect this to be a year of response. Directors should be asking "What are you *not* doing that you should be doing?" The key will be more transparency around these risks, along with the ability to prioritize them and understand how they are being funded.

Ken Athanasiou, vice president and CISO of AutoNation, believes identity and authentication management will be important in 2018, as both of these complex processes are a critical part of cybersecurity readiness. The authentication process in cybersecurity is considered one of the weakest links in computer security today. Authentication technologies such as biometrics, tokens, and others will elevate the ability to protect user credentials. Mr. Athanasiou explained that directors should understand "the current authentication process in place where it resides in the priority list."

Renee Guttmann-Stark, former CISO of Royal Caribbean International, presented another perspective on a 2018 trend. According to Ms. Guttmann-Stark, personal accountability will be a focus, and breaches are increasingly going to be associated with individuals. For example, Uber's chief security officer was recently fired after a massive data breach cover-up. Ms. Guttmann-Stark also commented on crisis communication and the need to classify the various types of incidents companies are going to see. As a director, which critical items should be shared with you? In the case of Equifax, directors were not made aware of the data breach until three weeks after the initial hacking.

Protecting the Company's Most Valuable Assets

Moderator **Nora Denzel** indicated that cybersecurity is not a "technology" problem; it is a business problem. She shared statistics such as:

- A criminal spends an average of 150 days in a company's network before being discovered.
- Over 50% of the time, it is someone outside the company (typically law enforcement) that informs the company they have been compromised.

In response, she recommended taking a simplified approach in the boardroom. Directors should know and agree on the answers to the following questions:

- What are the company's most valuable assets?
- Where are they?
- Who has access to them?
- How do you protect them?

In closing, Ms. Denzel and the panelists shared a final 2018 trend: resiliency. Companies are no longer focused solely on credit card issues. It has taken a few years, but companies are expected to continue to shift cybersecurity risk beyond information-technology planning and make this risk evaluation a normal part of the company's strategy.

Final Thoughts and Questions for Directors to Consider

- Ask management how cybersecurity is managed or governed in the company.
- Establish a good understanding of the tone at the top with respect to security.
- Challenge your fellow directors to elevate this discussion in the full boardroom.
- Do you have a good understanding of your insurance policy—what is covered, what is not, and how it works? Get a preplanning briefing from your insurance broker and a cyber-specialized lawyer.
- Cybersecurity risks are business issues, so discussion should include not only the technology experts but also the business, legal, and finance teams.
- Directors must understand the risks in the supply chain and understand how the company ensures that third-party suppliers with access to the company's network manage cybersecurity and how it's governed. Sometimes it's these third parties that are the weakest link.
- Ask how can emerging technologies such as artificial intelligence and blockchain enhance our cybersecurity posture?
- Don't delegate cybersecurity to the audit committee only. Request a quarterly cyber presentation to the full board on this important topic.

The NACD Florida Chapter would like to thank Northern Trust for supporting this event by providing the spectacular venue.

Evelyn D'An is an NACD Florida Board member and the Chair of the NACD Florida Advisory Board. President of D'An Financial Services, she is a senior financial advisor with comprehensive knowledge and proven leadership in corporate global finance, accounting, and operations. She is a director of Summer Infant, Inc. and active in non-profit organizations.