Cyber Risk Oversight 3.0

Major General (Retired) Brett Williams, Co-Founder of IronNet Cybersecurity, Inc., and Gerald M. Czarnecki, Chairman and CEO, The Deltennium Group, Inc., and experienced corporate director, shared insights on cyber risk and cyber security during the NACD Capital Area Chapter's November event at the Congressional Country Club in Bethesda. The discussion focused on questions directors can ask management to probe the company's cyber readiness, with context to help directors interpret the answers to those questions.

According to Czarnecki, technology and cyber risks are the biggest existential threats companies face, and the ability to ask questions is the most powerful tool directors have against these threats. Key areas addressed during the program include:

Cyber Risk as a Component of Enterprise Risk Management

Conventional wisdom includes cyber risk as an element of a company's overall risk profile; however, it is one of the most significant risks – one that could affect the company's reputation and financial bottom line.

Williams stressed that cyber intrusion is a certainty for most companies, so beyond confirming that the company has appropriate policies, the board should ask how management is implementing those policies. Further, directors should verify when the company has had:

- A third-party assessment;
- Penetration testing; and/or
- An outside audit or ISO certification.

Protecting the Crown Jewels

Because of the high likelihood of a breach, it is critical that a company identify the data most in need of protection. That is, since all files are vulnerable, the board should question which files are business-critical; what the company is doing to protect those files; and how much the company can afford to spend to protect those assets. According to Williams, data discovery –the question of "where is the data?" – can be the most difficult question to answer.

Additional area of exploration with management include:

- Who collects the data?
- How is the data collected?
- How much data is being retained?
- Is the crown-jewel data encrypted? At the device level? The device to cloud level? The cloud to device level?
    - Note that convenience to the user may become an area of possible push back from the CIO or CISO in the areas of encryption and authentication.
- Who has access to the critical data? How many third parties can access the data?

- Is the data backed up?

Regarding access, Williams pointed out that "real" hackers target the system administrators who have system configuration and data access, rather than the C-level. Czarnecki shared that companies may not have stringent processes to remove system or user access rights when an employee changes jobs or leaves the company. Williams concurred; after a hack of the Navy, the system showed one million users and passwords, yet the Navy only had three hundred and fifty thousand employees. Questions directors can ask in this area include:

- How do we manage passwords?
- How frequently are employees required to change passwords?
- What are the password requirements?
- What is the password management process?
- Who knows all the company passwords?
- Do we deploy multi-factor authentication?

A critical additional question relates to the company's backup strategy. What is backed up? Where is the back up? How do we know that we are backing up uncorrupted data? How do we access the backup data if it is needed? These questions are critical because, according to Williams, "Data backup is the number one defense for companies."

Breach Preparation

Part of preparation for a breach includes testing the ability to access backup data if need be; however, preparation also includes doing tabletop exercises, which must include top executives and even the board. Directors should ask when the last exercise was done. Assuming one has been done, the exercise should yield answers to key questions:

- Where are our gaps?
  - Where is more training needed?
  - Where should additional resources be deployed?
- Who will be the company's spokesperson?
- Do we have the right contacts?
  - FBI
  - Homeland Security
  - Law firm with expertise in consumer notification requirements
  - Forensics firm to determine what happened in a breach

Breach preparation should focus on the company's crown jewel data, be that healthcare records (currently the most valuable target); financial records; and even industrial control systems. At the conclusion of an exercise, gaps should be filled, then the company should enlist an outside expert to verify that those gaps have been appropriately filled.

Czarnecki stressed that with regard to all cyber discussions, board members should not be intimidated or deterred. "Ask questions until you are comfortable with the answers," he said. "If you don't understand or get the answers you are looking for, get an outside expert to help." Of course, directors can also turn to NACD's resources, including the organization's cyber handbook, cyber certificate course, or even "NACD Directors Daily" emails, which contain cyber-related materials on a regular basis.

The NACD Capital Area Chapter would like to thank the speakers, along with the chapter's sponsoring organizations, including Houlihan Lokey, for supporting this event.