NACD
NATIONAL ASSOCIATION OF CORPORATE DIRECTORS
MINNESOTA CHAPTER

Meeting Notes: Minnesota Chapter Roundtable

The Evolution of the Board's Role on Cybersecurity

October 25, 2017

A roundtable hosted by PwC.
Presenters: Michael Corey, PwC and Todd Bialick
Internal Technology Audit Services Leader – Non Financial Services
West Region Cybersecurity and Privacy Assurance Practice

Introduction by Lisa Hauser, PwC/NACD Minnesota Chapter Board of Directors

Michael began the morning with a discussion of what Cybersecurity used to mean at the board level and moved forward into the realities of the board level conversation today. The board conversation was strategy and resource allocation, along with other topics, and the CIO's role was tools and tactics. This equaled confusion and a lack of understanding of the real needs.

The issue is how to frame the conversation to fulfill the board's fiduciary responsibilities. Cybersecurity at its core is risk management. The primary question being, "What are we doing to manage the risk?"

A recent GSIS cybersecurity survey showed there is wide recognition of the importance of the issue of cybersecurity.

- 40% anticipate disruptions of operations as the result of an attack
- 44% have no cyber plan
- 48% no training in cybersecurity
- 54% have no plan for incident response

To rely on a smart CISO is no longer acceptable. Years ago, the concern was access to data and now it is the disruption of business.

A framework is needed to move forward. As a board member, how should I be thinking about this? There are three key questions they should be asking:

#1 What is the cybersecurity risk to our organization's business strategy?

#2 What about we doing about this risk?

#3 Are we doing enough?

Question #1 - What is the cybersecurity risk to our organization's business strategy?

Do we understand the risk at the strategic level? And, the most critical first step is understanding why cybersecurity is important to our business strategy.

- Look at the organization to determine the risk
- Show the process of understanding where the risks are
- Use the process to help determine the plan
- Choose where to put resources for maximum protection

The business conversation gives you the compass to implement. The CIO does the implementation.

Question #2 - What about we doing about this risk?

NIST and ISO are two of the most commonly used frameworks. Each has a built-in risk assessment process and can be tailored to match your organization.

- From a board perspective, establish the framework early and use as a basis to measure programs
- Focus on detect and respond controls in addition to prevent controls (which are always limited to human error)
- Focus on time to identify and show down a threat reactor

Responsibility: The CISO can report to the board (which is an IT through CIO movement). But this depends upon the organization and culture. There is no a black and white answer.

The three profiles of a CISO:

- Technologist
- Ex 3 letter government agency
- Risk-minded CISO (who needs to have all three profiles to be an effective CISO) and are usually very expensive

Question #3 – Are we doing enough?

The ultimate strategy questions are where we are and it is sufficient? There is a need for conversation on a quarterly basis (minimum) about the realities.

Once or twice a year, a group other than management (internal audit committee or board audit committee) should conduct an independent objective review of progress.

The ultimate goal is risk resilience and how to be more effective at it. There also should be a greater collaboration for sharing and learning.

Todd Bialick (U.S. Trust and Transparency Solutions Leader at PwC) briefly discussed AICPA, which is the reporting framework that wraps around the cybersecurity framework. Its purpose is to resolve “how do I tell others about what I’m doing.” Companies that want to release a report to others of compliance use AICPA.

Additional comments:

- Use of the Cloud increases the risk profile drastically.
- Internal users in an organization affect the risk level.
- AI and Robotics Machine Learning implemented into the business process make cybersecurity increasingly difficult to manage.