BOSTON BUSINESS JOURNAL

BEHIND THE BOARDROOM DOOR

# Public company directors talk cybersecurity, risk at the board level

May 8, 2019, 1:27pm EDT

Of all the responsibilities facing members of corporate boards of directors in 2019, cybersecurity ranks as one of the most challenging. What questions do non-experts need to know to ask of management? How can they tell if the answers are correct? Which board committee should "own" cyber?

The National Association of Corporate Directors New England chapter delves into these issues at its next event May 14 in Waltham with five experts: Retired Coast Guard Rear Admiral Mary Landry, a member of the USAA and Norwegian Cruise Line Holdings boards; Forcepoint CEO Matt Moynahan, former president of Arbor Networks and founding president of Veracode; Tom Reagan, Cyber Practice leader within Marsh's Financial and Professional Products (FINPRO) Specialty Practice in New York; David Farrell, assistant special agent in charge of the Counterintelligence/Cyber Branch of the Boston office of the Federal Bureau of Investigation; and moderator Steve Honig, corporate partner in the Boston office of the international law firm DuaneMorris LLP.

Here is a preview of the topic at hand:

**What do you consider today's best practice for boards of directors around cybersecurity?**

**Landry:** The task of cybersecurity oversight has evolved beyond delegating it to the chief technology officer or chief information officer. It has to be a shared responsibility at all levels of a company, including the board. Directors must find a way to focus on engaging in the strategic, high-level governance issues of import in the cybersecurity arena while each echelon of the company — from front-line employees to the executive committee to the board — clarifies its specific roles and responsibilities.

**Honig:** From a governance standpoint, each board needs to assess what it does and does not know, and must do the same with respect to its management. Each board needs to assign granular monitoring to a knowledgeable committee. The traditional relegating of such matters to the Audit Committee often is the wrong assignment based on skill-sets.

**Moynahan:** With a 95 percent success rate for the hackers and adversaries, industry has never seen such an imbalance between corporate spend and results. Today's failed approach to cybersecurity is responsible for putting adversaries in a more advantageous position, because it focuses more on protecting infrastructure and putting up walls to keep people out, as opposed to focusing on what's happening with the people on those infrastructures. Eighty percent of data breaches are caused by a company's own employees, either through malicious intent or their credentials being stolen through phishing attacks.

**How can non-tech-savvy directors be effective in providing cybersecurity oversight?**

**Honig:** It's important for them to be proud about being "dumb" by raising what stymies their current understanding. Few directors today have useful experience in managing this evolving risk. A significant part of cyber security is application of common sense–of which all directors are capable–along with asking what directors should expect management to be doing and what are best practices.