Deciphering Cyber for Your Board of Directors: Facilitating a Better Dialogue
Board directors are increasingly involved in cybersecurity risk management across a range of industries.

According to the 2017 What Directors Think survey by Spencer Stuart and NYSE Governance Services, 61% of directors indicated that their Chief Information Security Officer (CISO) meets regularly with the board to discuss cybersecurity. For BITS-FSR member firms, board engagement in cybersecurity is a regular occurrence. Most firms report that cybersecurity is a quarterly agenda topic for a board committee and the full board will be briefed at least once a year with many firms increasing the frequency. Many firms also report carving out specific board time for cybersecurity education on legal and regulatory requirements, cyber threats and incident response.

Despite regular board briefings, many CISOs and Chief Information Officers (CIOs) still report feeling like they have trouble connecting with the board and presenting information in an easily digestible form. Common concerns and struggles include the lack of a consistent set of metrics that allow for comparison over time and against other firms, the inability to quantify cyber risks, shifting threat landscapes, and varying levels of board expertise.

On July 25, 2017, BITS hosted a roundtable discussion among C-suite executives on board reporting. The meeting featured remarks from a current financial services board director and several CISOs who shared their experiences presenting and discussing cyber risks with board directors. The dialogue covered topics such as the board member perspective, what do you report to the board and how, the use of metrics and how to address challenging topics. The following summarizes the key discussion topics, which will be incorporated into the agenda for a similar October roundtable for independent board directors.

**Thinking Like a Board Director**

The secret to successful presentations is often knowing your audience, targeting your content and delivering accordingly. Boards are often composed of leaders from various industries, many of whom are likely not cybersecurity or technology experts. Better understanding board directors’ thought processes and how they are likely to approach a cybersecurity topic can help frame cybersecurity updates and encourage a robust dialogue.

Several CISOs as well as a current board director, highlighted the following things to keep in mind when speaking to the board on cyber risk matters.

- **Governance and Process** – Boards want to ensure the company has the right processes in place to evaluate and address risks. The board does not need to see the details of how you map all the existing cybersecurity frameworks and requirements to your internal controls, but will want to know that you have done that work. For board reporting purposes, using a heat map to categorize risks is helpful in fostering understanding and generating discussion.
**Talent Needs** – The board should understand there is a critical shortage of qualified individuals in the cybersecurity field and what it means for the firm. This poses a challenge in hiring and retaining qualified employees that will lead to elevated salaries and the need to recruit differently. Often times, talent shortages can lead to a need to outsource, necessitating a conversation with the board on how that will impact the firm’s risk.

**Risk Management** – The use of cyber specific heat maps showing significant risks was recommended as an effective way to facilitate dialogue around risk management and the CISO’s workplan. To the extent CISO’s can quantify the risks, identify program priorities and connect to the firm’s overall risk profile, it will make cyber risk more relatable and easier to understand and track.

**Third party reviews** of the firm’s cybersecurity posture were also noted as a good practice and something board directors can use to gauge progress and understand priorities. The board should hear the results and have a discussion on it, as well as what tools and resources are needed to address any gaps.

**Covering the News** – Cyber incidents in the news can be used as a good opportunity to help educate the board. Writing up a short (1-2 page) summary of the event, even if it does not affect your firm, is a good way to help board directors better understand the risks and put them in context to your firm. One CISO reported that they have a standard template that is used to draft a summary as soon as an event hits the news so that they are prepared should directors start asking questions.

---

**Metrics – Helpful or a Distraction?**

In talking to BITS/FSR members on board reporting, one of the most common questions is “What metrics do CISOs and CIOs use with their board directors?” There was consensus during the July roundtable that much of cyber risk management is subjective and that quantifying risk can require a lot of assumptions. There is no magic set of metrics and those in use never seem to scratch the itch. Yet, board directors will always ask for them, so what do people use?

Several roundtable participants reported that they select several metrics based on what the topic of focus is with the board. For instance, the time to detect an intruder or remediate an intrusion helps demonstrate operational effectiveness. The most useful metrics are those that show the effectiveness of the cyber program and objective progress against key improvement areas as opposed to just compliance with regulations.

---

**Connecting with the Board**

Similar to last year’s board governance roundtables, some CISOs reported they find it challenging to connect with directors and feel like they are not making progress in building upon previous briefings. Roundtable participants offered the following recommendations to build a trusted relationship and a solid foundation for cyber discussions over time.

**Everyone Loves a Field Trip** – Several roundtable participants suggested doing field trips with the board to help paint a picture. One opportunity noted to be particularly helpful with a lasting impact is a tour of the cyber operations center and a discussion with the staff responsible for defending the firm’s networks and systems. First hand interaction will help directors get a better sense of the risks the firm faces and how you tackle them.

**Show Business Value/Make it Relevant to the Business** – Another way to improve cyber briefings to the board is to align them to other business priorities the board may be discussing. For instance, how will moving to a single sign-on not only improve the customer experience, but also strengthen identity and access management? Or how can cybersecurity support cloud adoption? Connecting cybersecurity to other aspects of the business will allow the CISO or CIO to be seen as a business enabler.
Anticipating Questions – Most board directors receive a daily newsletter from the National Association of Corporate Directors (NACD) that includes articles on cybersecurity. One way to anticipate questions a board member may ask is to get a copy of the newsletter and review the coverage of cyber topics. NACD recently updated its guide for directors on cyber risk oversight, which some CISOs reported their directors have asked about. Given the regulatory requirements of financial firms, most CISOs already address the NACD recommendations, but directors may ask how you incorporate NACD’s guidelines as well. Being prepared for these questions and being able to talk about how NACD’s guidelines are a part of your risk management system is key to helping board directors integrate the information they receive with the context of the firm.

Board Directors Forum

BITS is hosting a cybersecurity meeting for independent board directors in October 2017 as part of our efforts to improve the cyber risk management dialogue. We have also provided bespoke board briefings to help educate directors and provide them context from across the industry to better evaluate cyber risks and activities.

The main themes from our C-suite roundtables will inform the content and dialogue for board-level discussions. Through those events, we will also gather direct feedback from directors that will be aggregated and anonymized to help C-suite executives as they continually seek to improve how they report on cybersecurity at their own firms.

For more information on these programs, please contact Chris Feeney, BITS President at Chris.Feeney@FSRoundtable.org, or Heather Hogsett, Vice President of Technology and Risk Strategy at Heather.Hogsett@FSRoundtable.org.


2 For more on BITS’ cybersecurity board governance program and last year’s work please see http://www.fsroundtable.org/bits/technology-risk-strateg