Cyber Risk – A Corporate Directors' Briefing
Webcast Q&A Summary

Cyber experts from Marsh & McLennan Companies and WomenCorporateDirectors hosted an engaging webcast on August 16th entitled "Cyber Risk – A Corporate Directors' Briefing."

The speakers were Catherine Allen, Chairman and CEO, TSFG; Director, Synovus Financial Corporation, El Paso Electric Company, and Analytics Pros; Kevin Richards, Global Head of Marsh Cyber Risk Consulting, and Elisabeth Case, Managing Director, Marsh Cyber Center of Excellence.

They provided valuable insight and counsel about:

- What board members need to know about the evolving cyber risk landscape;
- The increasing focus on response and recovery as essential risk management components, and directors' role in those functions;
- The value of cyber insurance as a risk transfer mechanism, and considerations for optimal insurance programs; and
- The right questions for directors to ask management, advisors and insurers in board meetings.

The speakers also addressed key questions from webcast participants, which are summarized here.

Evolution of Types of Attacks and Exposure

Q. How safe is the Cloud? What are your views on migrating business storage to the Cloud and the messaging of that as a security enhancement to shareholders? What requirements need to be added to Cloud computing contracts to better manage cyber security risks?

A. Security capabilities can vary widely across the array of Cloud providers. In some cases, Cloud service providers can deliver a heightened security posture, although it is imperative that a detailed assessment – both technical and commercial – be performed prior to deploying or migrating to Cloud-delivered services. Corporate counsel should be engaged to evaluate contractual covenants of the service level expectations.

Q. What is current single biggest cyber risk to corporations? What do you see as the most common shortfalls in companies when it comes to IT security?

A. While there isn't a single "silver bullet" for managing corporate cyber risk, from a macro-perspective, one area of concern is cyber operational governance – meaning the Chief Information Officer's (CIO) or Chief Information Security Officer's (CISO) ability to govern, influence, and manage the technological extended ecosystem. Whether through intended decentralization, strategic outsourcing, or simply leveraging myriad external service providers, many CIOs and CISOs have limited visibility on their technological estate. A recent article on CIO.com stated, "Gartner studies have found that shadow IT is 30 to 40 percent of IT spending in large enterprises, and our research at Everest Group finds it comprises 50 percent or more." Also known as 3rd party risk, this limited visibility significant hampers an organization's ability to understand and manage cyber risk.

Q. What industries are most vulnerable to cyber risk?

A. All industries are susceptible to cyber-attacks, and there are examples within every industry of cyber breaches. A great resource to research disclosed breaches is: *https://www.privacyrights.org/data-breaches*

Q. How should cyber risk be quantified to provide realistic risk exposure?

A. To be understood properly, cyber risk should be measured quantitatively in local currency, not in maturity scores. Board members need to understand the measured potential economic impact of a cyber event, not simply the adjectives describing the event. See more here: "It's Time To Quantify Cyber Risk Exposure".

Cyber Insurance

Q. What cyber insurance coverages are generally available?

A. Cyber insurance covers a broad swatch of first and third party exposures. First party coverages, like event notification or business interruption, reimburse an organization for the direct costs they incur to respond to or manage a breach, or the lost income they suffer as the result of a cyber event. Third party coverages provide defense and indemnity for an organization that may have incurred liability to others due to a cyber event.

Q. What risks are insurable? What should directors look for in insurance? What exclusions need to be understood?

A. There are a range of items that may impact the actual coverage of a claim, and while this list is not intended to be exhaustive, here are a few to keep in mind:
    - Prior acts / knowledge by C-suite or board
    - Bodily injury/property damage
    - Governmental acts, seizure, confiscation
    - Transfer of funds or loss/theft of money

Q. What is the right amount of cyber insurance?

A. There is no one-size-fits-all answer to insurance limits. Each company needs to assess their own risk exposure and understand their risk tolerance to make a determination of what insurance limits are right for them. The joint paper by Marsh & McLennan Companies and WomenCorporateDirectors, Cyber Risk Management: Response and Recovery, provides additional information on evolving approaches to cyber insurance.

Crisis Management and Incident Response Management

Q. What is the right role for directors in cyber incident response – what is the right level of involvement from the board and C-suite in both the planning and active response to a cyber incident/cyber crisis?

A. Board members and corporate executives need to play an active role first in ensuring that a formal cyber incident response plan and program is in place and tested on a regular basis. The plan should detail the roles and responsibilities of the various stakeholders based on the type and magnitude of the cyber event.

As part of this effort, identified board members and corporate executives should also invest time to participate in the planning and testing activities to align expectations.

With sufficient detail in the planning and testing activities, board members and corporate executives will better understand the process and participation requirements in the event of an actual cyber incident.

Risk Oversight

Q. What committee should oversee cyber risk? Should cyber security risk assessment oversight at the board level stay in at a committee level, or should it be at the full board level? What is the frequency and content of board updates?

A. While different organizations may vary on this approach, cyber risk would appropriately be actively discussed within the Risk Committee in conjunction with other enterprise risks.

However, unlike other risk areas, cyber risk is a newer subject that may need more frequent interactions than other, better understood risk areas. Initially it may be appropriate to discuss quarterly within the Risk Committee with, minimally, an annual briefing to the full board.

Q. What metrics do you monitor to track security program effectiveness? What are optimal "dashboard" type metrics for directors?

A. First, cyber risk should be measured and expressed quantitatively in local currency, not in maturity scores. Board members need to understand the measured potential economic impact of a cyber event, not simply the adjectives describing the event.

Program effectiveness can be presented in a number of ways, but should include at a minimum:

- A discussion of any cyber incidents – with associated losses (if applicable),
- Progress towards or achievement of regulatory/compliance objectives,
- Progress towards or achievement of targeted service level delivery – which could include the results of internal or external assessments or penetration testing activities, and
- Progress on completion of priority projects/initiatives.

Q. What are the qualities of an effective Chief Information Security Officer (CISO) now?

A. The roles and expectations for the CISO have changed over the recent years. The CISO has always been expected to understand the various cyber technologies, and similarly, the cyber threat landscape. Those areas remain true. But, the CISO in 2020 and beyond also needs to be well aligned with business leaders, product development, supply chain, manufacturing, and legal. The role of the CISO is more than protection of the IT function of the organization; the role should be to protect the business, its customers, and its shareholders. Additionally, CISOs need to have business savvy and executive maturity – which allows for effective communication across all levels of the organization.

Q. When should a board decide to seek external help for cyber risk guidance? Should a third party be engaged annually for a cyber risk assessment?

A. Boards need to have confidence that they – collectively – understand the subject matter sufficiently to direct their organization. With that, if the board feels it needs more insight, engaging an external party for experiences and guidance is appropriate. As a best practice, performing an independent annual cyber assessment provides an objective view on an organization's cyber capabilities.