Lead Director Network

June 2021

LDN

SUMMARY of THEMES

Board oversight of cybersecurity

Given the ever-increasing pace, scope, and sophistication of the cyber threats facing every company, managing cyber risk is one of a board's most challenging responsibilities. During a June 7 virtual meeting, members of the Lead Director Network (LDN) were joined by Eric Goldstein, executive assistant director for cybersecurity at the Cybersecurity and Infrastructure Security Agency (CISA), and Marianne Brown, former chief operating officer at FIS and current member of four public company boards, to discuss how boards can enhance their cybersecurity oversight.

This *Summary of Themes* provides a brief overview of the meeting. *For a full list of meeting participants, please see page 5.*

The proliferation of ransomware attacks has altered the cybersecurity landscape

Mr. Goldstein said that recent high-profile incidents have caused a dramatic change in how leaders are thinking about cyber risk: *"With two incidents in the past three weeks that resulted in material degradation to critical services on which Americans depend, there is a different tenor to this conversation than a few weeks ago."* The shift from attacks aimed at stealing data to ones focused on crippling a company's systems while demanding a ransom has significant implications for how a company addresses the risk. *"It is deeply important to exercise, document, and exercise some more about how the core business can keep going if there is a ransomware attack that takes down parts of the network,"* Mr. Goldstein advised. *"Are IT and the business working together to achieve this? Is the corporate network segmented from the operational network?"*

Responding to a ransomware attack requires swift action. Members discussed the importance of setting clear policies to enable a rapid response to a ransomware event. One director described the decision to pay ransom as a *"big, philosophical question"* that boards should discuss before a crisis happens; if a company might pay a ransom, it should also empower someone with authority to make the decision to pay. Mr. Goldstein affirmed that the US government discourages paying ransom, but he acknowledged the difficult position in which a ransomware attack places a company. Building resilience is crucial: *"If the business can keep serving its customers and ensure that revenue is more constant, it makes the decision of whether to pay easier,"* Mr. Goldstein said.[1]

[1] CISA's ransomware resources and guidance can be accessed at https://www.cisa.gov/ransomware.

Coordination among businesses and between the public and private sectors is a crucial element of cybersecurity

As part of its role in bolstering the nation's cybersecurity defenses, CISA promotes collaboration and information sharing among companies and between the public and private sectors. Mr. Goldstein emphasized that public-private partnerships should not supplant private-to-private cooperation. *"It is critical for companies to work together. Many of our cyber adversaries are using the same tactics to target multiple companies. The more companies share with each other, the better we will all do."*

He said that the government is hoping to foster more information sharing between sectors: *"It is not as common for private-private collaboration to occur among companies in different sectors. Government can bring cyber-risk information together across sectors."* He added, *"There is still significant asymmetry between sectors; energy and financial services are ahead of many others. We are focused on how to help mature cyber governance and oversight across sectors, modeled on what financial services and energy have done."*

In addition, Mr. Goldstein espoused the benefits of cooperating with CISA and other federal agencies: *"We have some degree of sensitive information that the private sector does not have. We are able to bring that information on specific threats or risks to a certain type of technology."*

The war for cyber talent can create additional opportunities for public-private collaboration

Given the scarcity of tech talent and the high salaries that skilled information security professionals can command in the private sector, members wondered how the government recruits and retains its team. *"We offer mission and we offer experience. We are not going to compete on salary,"* said Mr. Goldstein. *"Our pitch is that our country's most talented individuals should spend a few years helping their country and get great experience that is not easy to duplicate in the private sector."* Members observed the opportunity for public-private cooperation in this area. Mr. Goldstein also talked about the success of secondment programs in which companies send employees to work at CISA or government employees join private-sector cyber teams.

Third-party relationships require extra vigilance

Companies rely heavily on third-party providers for a range of critical services. While these relationships can drive efficiency and allow a company to focus on its core competencies, they can also complicate its approach to cybersecurity. One of CISA's roles, according to Mr. Goldstein, is *"to help companies improve cybersecurity for their third parties and their customers, which is increasingly important for all companies now. It helps avoid downstream compromises."*

Members noted that even if an individual company is not directly affected by a cyberattack, third-party relationships can *"bring those problems into your house."* One said, "*Thinking about dependencies opens up the world. What if a cyberattack takes down the power grid or transportation system, or disrupts steel production? How can one board or company be expected to consider all of that?"* Ms. Brown noted the importance of integrating such dependencies into incident-response and resiliency planning: *"Tabletop exercises provide an opportunity to look beyond the individual company and look at the wholistic universe."*

Boards are focused on enhancing their cybersecurity fluency

LDN members recognize the need for a board to stay abreast of an ever-evolving cyber-risk landscape and to maintain the necessary technical fluency to effectively oversee management's cybersecurity approach. Sometimes having cyber expertise on the board helps. Ms. Brown described her role as that of a translator: *"I take my operating-level experience as a fintech executive and use it to help the CISO* [chief information security officer] *to tell the story to the board in 'boardspeak.' I try to help make sure the reporting is not so complex that you can't see the forest for the trees."* Ms. Brown and members agreed, however, that the entire board needs to work constantly to improve its cyber literacy. Several directors noted that in recent years they have increased the cadence of training and educational opportunities for their boards in this area.

Effective cyber-risk oversight depends on good reporting from management

Ms. Brown encouraged directors to focus less on which framework a company follows for board-level cyber reporting and more on having a consistent, user-friendly framework or dashboard in place: *"What's important is not the thing you use, but that you use a thing."* Whatever form reporting comes in, boards need to be able to *"identify where you have risks and identify risk mitigants to the degree you possibly can. For example, it's important to look at vulnerability scanning and patching."*

She noted a number of questions boards can ask: *"How does the team identify attacks? What tools are they using to detect behavior? How do you protect assets through microsegmentation? How do you respond—do you have the ability to quickly shut things down to prevent spread? How do you recover?"* Mr. Goldstein said, "It's often *most effective to review the risks that could result from a degradation of the business' critical services. This allows for an equalizing of risks across a business and a more thoughtful weighting of risks and allocation of resources. Cyber should be baked into overall risk management."*

About this document

Summary of Themes reflects the network's use of a modified version of the Chatham House Rule whereby names of members and their company affiliations are a matter of public record, but comments made before and during meetings are not attributed to individuals or corporations. Guests, however, have given permission for their remarks to be attributed. Comments by guests and network members are shown in italics.

The views expressed in this document represent those of the Lead Director Network. They do not reflect the views nor constitute the advice of network members, their companies, or Tapestry Networks. Please consult your counselors for specific advice.

Meeting participants

The following Lead Director Network members participated in the meeting:

Marcela Donadio, Leader Director, Marathon Oil

Curt Espeland, Lead Director, Lincoln Electric

Glenn Hubbard, Non-Executive Chair, MetLife

Mel Lagomasino, Lead Director, The Coca-Cola Company

Lou Lavigne, Lead Director, Zynga

Steve Leer, Lead Director, Norfolk Southern and USG

Les Lyles, Non-Executive Chair, KBR

Jay Morse, Lead Director, AES

Oscar Munoz, Executive Chair, United Airlines

Henry Nasella, Lead Director, PVH

Pam Reeve, Independent Chair, American Tower

Pat Russo, Non-Executive Chair, Hewlett Packard Enterprise

Ted Samuels, Lead Director, Bristol-Myers Squibb

Doug Steenland, Lead Director, AIG and Hilton Worldwide