CYBER RISK BOARD FORUM
HIGHLIGHTS

The latest developments in cybersecurity and the proper role of the board was the focus of NYSE Governance Services' Cyber Risk Board Forum held on February 13 in San Francisco in partnership with RSA. Roughly 100 directors, CISOs, and other cyber governance experts met to hear cybersecurity experts, C-suite security executives, and representatives from the public and private sector discuss the most pressing issues related to cyber risk today. Key takeaways for directors and C-suite attendees were to understand the culture of compliance and security within their organization; to be aware of new and growing risks and liabilities associated with increasingly interconnected internet devices; understanding the benefits and risks of using cloud-based technologies; the need for cyber expertise on the board; and the growing need for dialogue between private and public sectors to address cybersecurity.

NYSE Governance Services

CYBER RISK BOARD FORUM

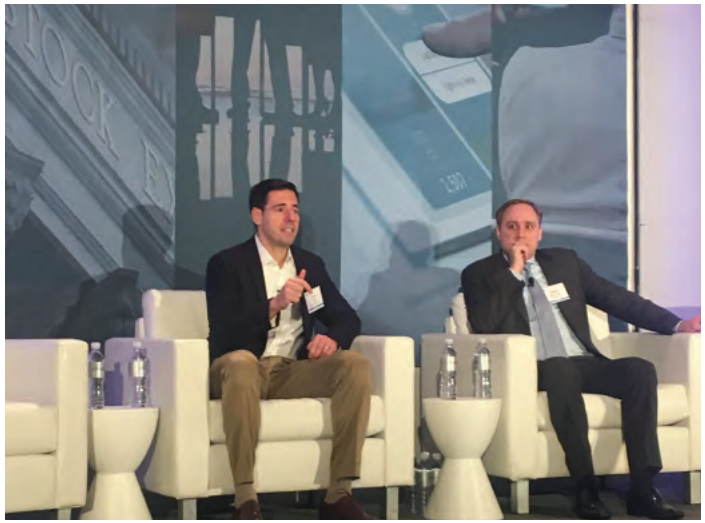
RSA President Rohit Ghai welcomed attendees, saying he was pleased to see directors and C-level officers taking a strong interest in proactive cyber risk strategies. “Cybersecurity is squarely a business topic today, and when you look at all the possibilities of what can happen, you must know that the downside risk is very real,” he said.

Kicking off the event was an information-packed keynote centering on the relationship between governmental and independent agency investigations of cyber incidents within private companies. John Carlin, former assistant attorney general for national security within the Department of Justice, was joined by Dmitri Alperovitch, cofounder and chief technology officer at Crowdstrike, an incident response and cloud solutions services company. Both speakers offered lessons learned from recent, high-profile breaches such as Sony and Target. In the case of Sony, Carlin noted, there were several new developments that changed the game—namely the fact that North Korea used the situation to not only threaten to steal data but to infiltrate a company and use scare tactics on its employees.

“Sony responded in the right way,” said Carlin, who said it was very important that its executives knew who to call in the government ahead of time. “If you don’t know the name and number of who to call, you are not prepared,” he warned.

Carlin and Alperovitch offered several takeaways for preparing for a cyber breach incident:

- do a compromise assessment immediately to ascertain where you are most vulnerable;
- try to learn where data resides inside the organization;
- understand what your data assets are;
- think like an adversary; and
- ensure there are the right business owners for the risk.



CYBER RISK BOARD FORUM

Since cyber oversight has risen to the ranks of a governance issue today, the next session featured a panel who discussed how to ensure a board has the proper expertise to manage cyber risk as part of the business strategy. Joining the discussion were Tony Buffomante, principal and Cyber Security Services US leader, KPMG; Daniel Cooperman, Technology & Cybersecurity Committee chair, Molina Healthcare; and Jerry Perullo, chief information security officer, Intercontinental Exchange.

The panel offered perspectives on the skills and background necessary to understand and monitor cyber risk as well as the security officer reporting structure, which helps ascertain where ownership of cyber risk falls. “It is important for the CISO’s reporting structure to make sense for every company,” Perullo noted, explaining that there is not a one-size-fits-all answer. He also noted that in terms of analyzing and identifying cybersecurity vulnerabilities, “data theft is one small sliver.” Additional considerations such as reputational risk and operational downtime are equally if not more damaging to a corporation that has undergone a cyber breach.

Debunking the notion that cloud solutions might be less secure than physical onsite security, the following panel offered tips and good practices for ensuring a company has the appropriate safeguards in place. Debating these topics were Alissa Johnson, chief information security officer, Xerox; Dave Palmer, director of technology, Darktrace, a maker of enterprise immune system technologies; and Matthew Prince, co-founder and CEO of Cloudflare, a web performance and security company.

CYBER RISK BOARD FORUM

The afternoon sessions launched with a lively keynote panel featuring Michael DeCesare, president and CEO of network security firm Forescout, who was joined by Robert Herjavec, CEO and founder of the Herjavec Group, a cybersecurity protection services company. Herjavec, more widely known as one of the primary "sharks" from the television show, Shark Tank, offered insights on cybersecurity trends and how companies can take steps to protect themselves. In particular, beware of "spikes in cyber breaches" expected to hit government organizations and the health care industry, Herjavec noted. Finally, with all that is known about the likelihood of a cyber breach today, "It surprises me how many large enterprises don't have a remediation plan," Herjavec said, stressing the importance of not only being prepared for an attack, but what to do afterward.

One of the most fluid areas in the realm of cybersecurity is that of ongoing regulation, legislation, and policy. The forum boasted a panel of top experts in the US today to discuss these leading-edge issues: Michael Daniel, former special assistant to the president and cybersecurity counselor, National Security Council; Matthew Eggers, executive director of cybersecurity policy, US Chamber of Commerce; and Rob Knake, senior fellow, Council on Foreign Relations.
The panelists noted that in this environment, companies cannot sit on their laurels. And frankly, they agreed, the punitive effects of a cyber breach are simply not enough to change protection behavior. "There needs to be incentives in place for companies to get cybersecurity right," Daniel said.

CYBER RISK BOARD FORUM

Board reporting was the topic of another afternoon panel session that delved into which reporting structures often work best and why, as well as how to make sure directors get the most relevant information to make decisions on cybersecurity oversight. Led by Erica Davis, senior vice president and head of specialty insurance products for Zurich, NA, the panelists, including Melissa Hathaway, president of consulting firm Hathaway Strategies, along with Sheila Jordan, senior vice president and CIO of cyber protection software developer Symantec, discussed the current threat environment and best practices for board oversight. They noted that the board should be asking for reports about cybersecurity risks—legal, financial, and operational—on a quarterly basis, and also that it's a good idea for boards to occasionally have an executive session with the CISO.

The penultimate session of the day involved an interactive case study centering on incident response and communication plans, energetically led by Nicole Bucala, principal of operations and strategy with RSA Security, and Roland Cloutier, vice president and chief security officer, ADP. Cloutier and Bucala walked the audience through a sample business disruption emanating from a cyber breach and analyzed several frameworks to be used to evaluate moral, ethical, and legal responsibilities during incident response. They delved into the various ways in which reputational harm stems from a breach, as well as the ways in which companies can mitigate losses in confidence from clients, employees, and shareholders.

Completing the forum was a final panel titled "Channeling Success through Security." which emphasized positive ways to implement cyber practices into the fabric of an organization. With an eye toward opportunities rather than risks, Michelle Dennedy, chief privacy officer, Cisco, and Jim Pflaging, principal and business strategy practice leader, The Chertoff Group, offered ways in which harnessing the power of a company's cyber strategy can drive new business and raise the awareness of customers and clients about competitive advantages. Said Phlaging, "Cybersecurity should be the centerpiece of how a company digitally revolutionizes its business going forward."