Safety in Numbers: Cybersecurity 101 for the IRO

March 15, 2016

Panelists: **Steven H. Shapiro**, Partner, Krasnow Saunders Kaplan & Benninati
Andrew Liuzzi, U.S. Crisis Lead, Data Security & Privacy Group, Edelman

Moderator: Ruth Venning, Treasurer, NIRI-Chicago; former director of IR at Hospira, Inc.

Key Takeaways

- Cybersecurity has become one of the most pressing issues for companies. Cyber incidents are on the rise, and a data breach in the United States costs an average of $6.5M – not to mention reputational damage it can cause. And the after-effects of a cyber breach can be devastating: Steve Shapiro cited a sobering statistic that 60 percent of small businesses that experience a cyber-attack are out of business six months later.
- The panelists agreed that it's not a matter of "if," but "when" a company will experience a cyber breach. It's therefore important for companies to manage cybersecurity from multiple perspectives, ranging from mitigating the various risks (business, operational, financial and corporate governance) to protecting the company's brand and reputation.
- Understandably, institutional investors are increasingly asking about companies' cybersecurity programs. How can an IRO be prepared for investors' cybersecurity questions – or worse, an actual breach? Know what your company is doing about cybersecurity. Know your board members' qualifications related to data security and their role in its oversight. Know how your company trains employees about the risks – because the greatest exposure to cyber risk is not hackers but employee negligence. On your part, protect the sensitive data you deal with. Then be prepared. Make sure your company has a cybersecurity incident response plan in place before an incident occurs – and have an IR cybersecurity communications strategy for answering investor questions.
- Shapiro discussed cybersecurity from the corporate governance perspective, noting that cybersecurity is the No. 1 concern of board members and general counsels. He highlighted the challenges managing cybersecurity poses for companies and the growing trend of cyber incidents. It usually takes only minutes for an incident to occur, he said, but it can be months before it's discovered – usually by the FBI. While there's no such thing as perfect security, it's critical to have a robust cybersecurity program – and to ensure that the board is trained and involved in the program oversight.
- In discussing cybersecurity from a crisis-management perspective, Andy Liuzzi agreed with the importance of planning. Proactively developing a crisis communications plan can save the company money and reputational damage in the event of a cyber breach. Liuzzi presented steps to create a plan: 1) identify the internal and external members of the team (keep it lean) and designate the chain of command. 2) Socialize the plan with key internal stakeholders. 3) Identify and foster relationships with key influencers such as state regulators and policymakers. 4) Determine your lobbing, forensic investigators and legal partners in advance. 5. Conduct simulated crisis exercises regularly to give team members a chance to practice the plan as well as to identify potential gaps in the response process or communications strategy.
- The panel discussed current investor disclosure practices around cybersecurity. A handout showed how several companies considered "best-in-class" for proxy statement disclosure addressed cybersecurity in their proxy statements.
- Finally, both Shapiro and Liuzzi emphasized the importance of handling sensitive data properly, given that unintended employee – or board member – negligence can result in cyber breaches. Don't email sensitive data without protecting it (e.g., with passwords) and be sure you use appropriately protected devices for work-related emails and documents.

– Ruth Venning