IDC Independent Directors Council
Promoting Excellence in Fund Governance

ICI VIEWPOINTS

JUNE 12, 2015

Cybersecurity: Managing Risk in an Increasingly Connected World

By Todd Bernhardt

It's increasingly obvious that we live in a world where cyber threats are evolving quickly and will remain persistent. But though such risks can never be eliminated, they can be managed, said panelists at ICI's Operations and Technology Conference, held in conjunction with the Institute's General Membership Meeting May 6–8 in Washington, DC.

A capacity crowd gathered on the morning of May 7 to consider the question expressed in the panel's title: "Cybersecurity: Advanced Persistent Threats to Zero Day Exploits—What Are We to Do?" Answering that question were five information security experts, led by Ellen Rinaldi, principal for enterprise security at The Vanguard Group, who moderated the panel; David Joire, senior counsel in the Division of Investment Management, Chief Counsel's Office, at the U.S. Securities and Exchange Commission (SEC); Mark Nicholson, a principal at Deloitte & Touche; Ronald Rowe Jr., senior advisor to the National Intelligence Officer for Cyber Issues for the National Intelligence Council's Office of the Director of National Intelligence; and John Watters, chairman and CEO of iSIGHT Partners.

Responding to a question from Rinaldi about how to prioritize efforts in a world where "100 percent cybersecurity is impossible," Nicholson said that his firm groups cyber efforts into "three primary buckets: being secure, being vigilant, and being resilient." Though external threats are always important to guard against, he explained, it's also "important to look at your internal organization and possible threats, especially in large organizations."

Examples of external threats include state actors, who sometimes attempt to access and exploit systems as part of ongoing espionage efforts, or who attack organizations in an effort to damage their systems or brand (the panelists pointed to the alleged attack by North Korea on Sony Corporation as an example). Internal threats could include employees with criminal intent ("there are a lot of things that can be monetized, far more than we usually consider," said Rowe) or "hacktivists" trying to achieve ideological goals.

The important thing, said Watters, is to examine your organization for vulnerabilities, keeping in mind that "all connections are access points for an adversary to get in." The next step then, he explained, is to prioritize. "You have to shrink the problem—allocate resources to the threats that are most dangerous and could have highest impact. This helps you effectively manage risk on a per-dollar basis."

Plan, Test, Adjust, Repeat

Being prepared means having a plan, of course. And having a plan means involving everyone in the firm, at every level, the experts agreed.

As the regulator on the panel, Joire focused on the importance of the role played by a firm's chief compliance officer (CCO). "There's a compliance aspect to cybersecurity—various rules that people need to follow—and the SEC is highlighting that," he stressed. "The CCO should engage in a dialogue with the cybersecurity team and with management, to break down barriers between them."

Watters emphasized that though the government has a role to play in cybersecurity, it's more limited than some might expect. "I think the government should be tasked with providing frameworks, but they're not going to actively protect you," he said. Rowe agreed, adding with a smile that "there's a perception that we have Seal Team 6 on standby. But there's no Jack Bauer who's going to save the stock exchange."

Because of this, it's important to create a sense of personal responsibility for cybersecurity among all employees, said Nicholson. "Often, it's an inside user who's taken advantage of," he explained. "So it's important to educate and train employees about the risks....You need to ensure that there's a culture of accountability throughout the firm."

A trained workforce helps an organization plan for cyber incidents and respond to them more quickly than it otherwise would be able to, said Rowe. Having a plan in place early—and testing it often—is key, he explained: "You don't want to be testing your response plan under stress. Everyone in the firm needs to be involved and ready to go."

Watters agreed, saying, "When you have a plan in place and respond quickly, it reduces the value of any info that hackers are able to steal."

"We conduct 'cyber war games' where we practice what happens in the event of a cyberattack on Wall Street," Nicholson added. "This helps you test your communications, to see if all the necessary parts of the firm are working together to respond."

Protecting Networks from the Outside In

The cyber experts also agreed that organizations need to focus on threats that leverage outside connections as access points, including mobile devices used by employees and network connections shared with vendors and other third-party service providers. "Apps help a lot of people, but they create a lot of opportunities for exploitation," Rowe said. "Mobile is a necessary risk—but you have to make people aware of the dangers....A compromised mobile device can lead to other access."

Watters agreed that mobile devices "dramatically increase the opportunity of bad actors getting in," warning that "there's no such thing as a hardened perimeter anymore."

"And with the proliferation of the 'Internet of Things,' it's only going to get worse," Nicholson reminded the audience. "We need to be vigilant and diligent. We're not going to be able to stop it, but we need to keep up with it, to the extent possible."

Nicholson also stressed to the crowd that companies need to look at all of their vendor relationships, in the context of the role they play in a firm's overall business processes, to ensure—through risk-assessment surveys and other means—that vendors are not providing a means for hackers to gain access to the firm's computer systems. These expectations should be reflected in any contracts that firms have with vendors, he and Rowe said. "If you're going to hire someone, you have to hold their feet to the fire in their contract," Rowe explained. "They have to share your security."

Help Is Available

The scope and scale of cyber threats can seem intimidating, the panelists admitted. But "the financial sector has done a good job at protecting data," Rowe said. He and the others gave an overview of resources that can help companies learn about threats and how to guard against them.

Joire pointed out that the SEC had released cybersecurity guidance in April, while others on the panel talked about other guidance and security frameworks released by regulators and government agencies, including the NIST Cybersecurity Framework.

Rinaldi reminded the audience that ICI has created an Information Security Resource Center containing links to a wide range of resources. The center also includes a comprehensive list of questions that a firm should consider when assessing its cybersecurity programs, as well as its vendors' programs.

Finally, as she wrapped up the program, Rinaldi highlighted ICI's cybersecurity forums, which enable attendees and participants to share information on the latest threats and vulnerabilities while gaining insights on best practices for the industry. The first forum was held last December, attracting a capacity crowd, and two forums are planned for the near future: one on July 14 in London, and one on November 5 in Washington, DC.

For other GMM highlights, please visit http://gmm.ici.org/gmm/2015/15_highlights.

Todd Bernhardt was senior director of public communications at ICI.
