The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE
Washington, DC // Brussels // London // www.ici.org

ICI VIEWPOINTS

MAY 7, 2013

GMM Panelists Share Tips on Strengthening Cybersecurity

By Andrew Gillies

Cybersecurity gained prominence as a topic of discussion at ICI's General Membership Meeting (GMM), held last week in Washington, DC. "Hugely important," said Mary John Miller, the Treasury Department's under secretary for domestic finance, in her GMM remarks. Likewise, Securities and Exchange Commission Chairman Mary Jo White told GMM attendees that addressing online vulnerabilities must be "a constant focus for both the regulators and the broader business community."

That focus also was on display May 3 at the Operations and Technology Conference, where a panel of technology experts explored the origins and implications of cyberattacks. Panelists also provided the audience with cybersecurity advice, including the following pointers.

1. Check Every Link in the Chain

"Any of your service providers could be attacked and could leak data," said Stewart A. Baker, a partner at Steptoe & Johnson LLP. Baker, who helped formulate U.S. cybersecurity policy as assistant secretary for policy at the Department of Homeland Security and as general counsel of the National Security Agency, urged attendees to get assurances from all service providers about data security arrangements.

Panelist Avivah Litan, vice president and distinguished analyst at Gartner Research, agreed that understanding the security of service providers was essential. "We're only as strong as the weakest link," she said.

2. Don't Discount Low-Tech Threats

Cyberattacks can have very sophisticated sponsors (e.g., nation-states such as Iran and North Korea) using advanced technology. Even so, Litan cautioned, no one should discount the danger from more low-tech methods of attack, particularly those involving old-fashioned infiltration via employees who can—knowingly or unknowingly—provide access to networks.

In one instance, she recounted, hackers targeted an organization by befriending workers at a gym near its offices. In another, a print room clerk was paid off. "We spend a lot of time on these more exotic kinds of actors coming in through cyberspace," said Litan, who worked as a director of financial systems at the World Bank. "We forget sometimes about the guy in the print room." Thus, Litan stressed the value of a strategy involving multiple layers of security.

3. Educate

Among those layers, of course, should be robust employee education around cybersecurity. John Shea, chief information officer at Eaton Vance Management, emphasized that education about cyberthreats shouldn't just focus on what employees can or can't do—it also should clearly explain *why* such steps are necessary.

As an example, he cited the relatively recent realization that portable flash drives, although convenient, can carry computer viruses or malicious programs. "When you say, 'Hey, I'm not going to let you plug a USB device into your PC anymore,' having an education of what the risks are reduces the sting of taking things away," he said.

Education also involves conveying the nature of the threat. Baker suggested that cybersecurity should be described as nothing less than combat. "You are engaged in a fight with people who want what you have, and who will use a variety of tactics to take it away

from you," he explained.

4. Make Stuff Up

With people sharing more and more personal information via social networks such as Facebook and LinkedIn, password protection becomes a greater challenge. A mother's maiden name or a former teacher's name, for example, is easier information to come by these days. Shea had a simple piece of advice on this topic—invent. For example, if a password challenge is a pet's or former teacher's name, make one up.

5. Keep the Old

Use of technology to streamline and automate processes has greatly improved the fund industry's efficiency—and will continue to do so. But Litan suggested that some back-end fund industry checks that may appear antiquated—such as those involving phone calls or written notifications that flag account activity—can be a "saving grace" when it comes to cybersecurity. "Keep those age-old processes," she said. "They work really well."

The panel was moderated by Daniel T. Steiner, executive vice president and general counsel for ICI Mutual.

Andrew Gillies is managing editor of policy writing at ICI.
