Focus on Funds: How Can You Benchmark a Cybersecurity Response Plan?

Focus on Funds

How Can You Benchmark a Cybersecurity Response Plan?

Funds don't often have the opportunity to compare notes on response plans, but a recent ICI conference brokered such a dialogue. In the March 17, 2017, edition of *Focus on Funds*, Peter Salmon, ICI senior director, operations and technology, discusses the diverse perspectives of panelists.

Transcript

Stephanie Ortbals-Tibbs,ICI Director, Media Relations: For cybersecurity professionals, instant response planning is a critical part of the job. So recently, they came together to compare notes, as I learned from ICI's cybersecurity expert, Peter Salmon.

Peter Salmon, ICI Senior Director, Operations and Technology: The purpose of having the [incident response] panel is to show the interconnectedness between the different roles within an organization and get the different perspectives on what goes on during an incident, when do we involve certain individuals, certain functions, internal and external. And the purpose is to reinforce with everybody that you have to have this plan in place and exercise before something goes wrong—because during an emergency, it's not the time to figure out what steps within your procedures you should be doing, who you should be notifying, who did what, when, and why. So this sort of highlights all of the steps and considerations that firms need to take into account when there is a problem.

Ortbals-Tibbs: So this was really a rare opportunity within the industry for asset managers to take a look at other companies' plans, compare notes, and see how theirs stacks up.

Salmon: Absolutely, the exchange of ideas is incredibly valuable. People come at this with different years of experience, different backgrounds, and so it's just a healthy exchange of people facing the same challenge and how do they approach that, and how to they mitigate?

Ortbals-Tibbs: You had a lot of different perspectives in the room and on that panel.

Salmon: Absolutely, and communications is a key part of it, because depending on the nature of the incident there's going to have to be communications with investors, with the public generally, and perhaps with other entities, so you're going to want that planned out and the communications professional needs to be involved in these discussions.

Ortbals-Tibbs: And the very fact that you had a communications professional on the panel indicates that this was not your typical lineup at a cybersecurity conference. You were really having people think much more broadly about this issue and the people they have involved in their response plan.

Salmon: Well, for me it's a reinforcement of what the Institute has been doing for a while, which is highlighting the key role that law enforcement plays in incident response plans. And it's not a question of calling them when they don't know who you are, because you'll just get a switchboard number and they won't know how to direct your call. You need to have a relationship established before an incident takes place and we've gone out, not only here in the United States but abroad, and reemphasized that and actually introduced individual agents to our members so that they can include that specific agent's name and number in their incident response plans.

Additional Resources

- Highlights from ICI's 2016 Cybersecurity Forum
- ICI Information Security Resource Center
- *ICI Viewpoints* Series: Cybersecurity at Work
- *Focus on Funds:* How Should Fund Boards Engage in Cybersecurity?
