The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

VIDEO

February 10, 2017

Focus on Funds: To Strengthen Cybersecurity Plans, Think Like a Hacker

Focus on Funds

To Strengthen Cybersecurity Plans, Think Like a Hacker

In the February 10, 2017, edition of *Focus on Funds*, SafeBreach CEO Guy Bejerano discusses the most effective approaches to coping with cybersecurity threats.

Transcript

Stephanie Ortbals-Tibbs, ICI Director, Media Relations: How much money should you spend on your cybersecurity? That's a million—often multimillion—dollar question.At ICI's recent cybersecurity conference, I got some fresh insight from one of the experts.

Guy Bejerano, CEO, SafeBreach: So, people think about spending money on security and the question is, how effective is it? And so, if you spend a lot of money, how do you actually know that money will prevent the next breach? How do you know how good your controls are? And if tomorrow something will happen, how do you know that those controls that you already put in place and invested money in, will actually come to play in the right way?

Ortbals-Tibbs: So how can companies be more effective in their risk assessment?

Bejerano: So, the first thing would be is to think like the adversary. If you bring the adversary to the game, you've already built your security program. Now bring the adversary, and see how it plays. The wrong thing to do is actually to wait for the attack to happen. And if you do that, you're already too late.

Ortbals-Tibbs: And since it may not be natural for everyone to think like a bad guy, how do you need to do that? How do you begin to look around corners to see risk?

Bejerano: So it's more on realizing how an attack looks like—what are the phases, and what are you trying to protect from happening? And if you understand those two elements, and you can play them—and there are multiple ways to play them—then you're actually doing the right thing.

Ortbals-Tibbs: We've talked about risk assessment. What about risk mitigation? That could be a pretty tough fight. How do you fend off attacks?

Bejerano: Correct. I think that the challenge is—because a lot of people are focusing on the hacker's strength point and not on his weakness—and if you look at how hacking has changed over the years, it became more sophisticated, more complex, and that's actually its downside. So by really understanding how the flow of the attack works, you can find those weak spots where *you* have the advantage. And so not focusing only on where the hackers are stronger, but also where you are stronger, and just focusing on mitigating those parts, will actually break the entire chain.

Ortbals-Tibbs: So many times, too, what people have begun to talk about is that it's maybe also timeto move beyond the question of avoiding an attack but also coping with them. What are your thoughts on that issue?

Bejerano: I think it's a great mindset. So, if you just stay away from trying to prevent everything—which you will never get 100 percent success in—and you're focusing on how can I actually reduce the impact, how can I, as you said, live with the attack but make sure that the impact will be such that my business can absorb it? And that's the main thing.

Ortbals-Tibbs: So, a final question based on the discussion today. What's one action item that you would identify for people in the fund industry to think about doing?

Bejerano: First of all, validate your assumptions. So, either you hire your hackers, you know, take an automation platform like SafeBreach, or any other means—just validate your assumptions, and then start from there.

Additional Resources

- Highlights from ICI's 2016 Cybersecurity Forum
- ICI Information Security Resource Center
- *ICI Viewpoints* Series: Cybersecurity at Work
- Video: With Cyberthreats, Preparation and a Quick Response Are Key