The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

VIDEO

November 13, 2015

Focus on Funds: With Cyberthreats, Preparation and Quick Response Are Key

Focus on Funds

With Cyberthreats, Preparation and Quick Response Are Key

The November 13, 2015, edition of *Focus on Funds* examines the need for constant vigilance in detecting cyberthreats, and advice about how best to counter them.

Transcript

Stephanie Ortbals-Tibbs, ICI Director, Media Relations: Cybersecurity is increasingly the business of all of those in the asset management business and at ICI's most recent cybersecurity conference in Washington, DC, I gained some fresh information and insights from one of the leading experts in this field, beginning with some numbers that should get everyone thinking.

Tony Cole, Vice President and Global Government CTO at *FireEye*: I'll tell you, from my global travels, one of the challenges we see across the board is, today, we see an average time from when a system is breached, so until they are actually notified or find a breach, is on average 205 days. So when you see data exfiltration take place sometimes in minutes or hours, 205 days is an enormous amount of time. And then on the other side of that, 67 percent of the time they never find that breach themselves. Their local law enforcement, so a computer emergency response team, or another organization seeing anomalous activity coming from their network towards theirs, will notify them. So those numbers tell us that we're not catching those breaches today.

Ortbals-Tibbs: Any suggestions then for what asset managers should be thinking about, a priority list for them as they go forward and try to continue to work on this?

Cole: Yes, they need to understand that, one, sooner or later they will get breached—it just happens. You can't prevent all of it because we have an adversary with evolving tactics and tools and processes. They're going to get in sooner or later. So can you identify them right away so you can stop them from exfiltrating data and then ensure that you actually closed the hole they used to get in, and then find the additional systems they may have comprised as well. So threat attribution, so an intelligence related to that is critically important so you actually understand what the adversary is trying to do and how can you actually find other activity they've had inside your network.

Additional Resources

- ICI Information Security Resource Center
- Video: ICI Global Cybersecurity Conference Highlights
- Video Highlights: New Cybersecurity Coordination