The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

VIDEO

February 17, 2017

Focus on Funds: A Noted Hacker Shares Security Tips

Focus on Funds

A Noted Hacker Shares Security Tips

In the February 17, 2017, edition of *Focus on Funds*, Kevin Mitnick—known as a "white hat hacker" for his work helping companies vet their cybersecurity—examines some trends in cybersecurity, as well as how companies can prepare.

Transcript

Stephanie Ortbals-Tibbs,ICI Director, Media Relations: What does one of the most noted white-hat hackers want you to know about cybersecurity in our industry? Recently I had a chance to talk with Keven Mitnick.

Keven Mitnick, CEO, Mitnick Security Consulting: Well, it just keeps on going. It's kind of like a cyber arms race. As the hackers get smarter and create new methods of getting into systems, the defenders—businesses—innovate and think of ways to try to protect the business, and then again, the hackers become more innovative, so it's this constant cat-and-mouse game, and it keeps on going.

One of the toughest things to do today is detect and eradicate malware. What's malware? Malicious code. There are not really any good products out on the market that we can't defeat—and that's pretty scary, because if we can't defeat it, when hackers are breaking into your business, and if they use specialized malware, you're not going to catch them either.

Ortbals-Tibbs: So, you spend a good deal of time talking about "hacking the human"—how one person's ordinary, everyday activities like opening a PDF, could cause a tremendous amount of mischief.

Mitnick: Imagine a customer, or a brand-new customer that wants to establish a business relationship, and as part of an email or evaluation they send you a mutual non-disclosure agreement, which is normal. It's a PDF file, and once you open up that PDF file, it exploits your machine.

Ortbals-Tibbs: Kevin, you engage with lots of different industries, and I'm curious to see if you think the fund industry has any different issues when it comes to hacking than other

industries.

Mitnick: Well, it's a target-rich environment, so they have to meet a higher standard and they must manage their risk somewhat differently. But it's usually the same across the board, of how the attackers get in. You have to have good defense, you have to have good detection, you have to have a way to remediate a problem if one exists.

And you have to be very proactive, not reactive, about it, because when something bad happens, you don't want to be scrambling. You want to already have a process in place to deal with it. So, it's very dynamic, it changes every day, so you need to be on top of the game. Or you need to outsource your security to a company that does keep up on their game.

Additional Resources

- Highlights from ICI's 2016 Cybersecurity Forum
- ICI Information Security Resource Center
- *ICI Viewpoints* Series: Cybersecurity at Work
- *Focus on Funds*: To Strengthen Cybersecurity Plans, Think Like a Hacker
- "A New Security Vulnerability": Additional Insight from Kevin Mitnick

---