The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

VIDEO

August 12, 2016

Focus on Funds: Learn About the Latest Emerging Cyberthreats

Focus on Funds

Learn About the Latest Emerging Cyberthreats

The fund industry continues to be vigilant about safeguarding fund and investor information, yet staying ahead of new threats is a constant challenge. Learn more in the August 12, 2016, edition of *Focus on Funds*, which features key takeaways from ICI's recent cybersecurity conference in London.

Transcript

Stephanie Ortbals-Tibbs, Director, ICI Media Relations: Defending against ransomware, managing the emerging risk to the Internet of Things and building a global network of cybersecurity professionals—these were just a few of the topline trends on the agenda at ICI Global's latest cybersecurity conference in London. Here are some key takeaways.

Tony Cole, Vice President and Global Government CTO, FireEye: It's a scary, new trend that we saw really a significant uptick in last year. So, on our m-trends 2016 report, looking across 2015, where we're seeing more and more FIN—it's the category of how we track these people (financial services, but FIN)—attackers actually go through and attack hospitals, healthcare organizations, banks, and other organizations where they can encrypt the data and then hold them for ransom. So they either encrypt it and hold them for ransom or release some of the data to prove they had access to the systems.

Ortbals-Tibbs: So, what should people in a business like ours do? How should they brace themselves for this trend?

Cole: I think one of the things you definitely have to do is you have to work harder on understanding attribution. Who are the potential people who want to attack you? And what are you doing to ensure that you're safeguarding: knowing your assets, safeguarding your assets by making sure you have updated operating systems—the latest versions of them—that they're patched, and then you're actually looking at threat intelligence, as well, as a component of how to understand who is going to attack you and how you ensure that you're prepared for that.

Ortbals-Tibbs: Can we also talk about another door that might be open inside organizations that they're not thinking about and that's this growth in, what you call, the

Internet of Things (the IOT) and the way that could be opening up new vulnerabilities for companies. Give us some examples of what those things are, if you could, and how that could play out.

Cole: Sure. We're standing here in London and it's a great area to talk about it. If you look around here, there are cameras everywhere. While many organizations today have those cameras or IP-enabled cameras that actually feed the data back, those can be IOT—Internet of Things—devices. And if you don't plan that into your infrastructure with security in mind, then you have potentially set up a back door into your infrastructure. And that's just one piece for a system that's moving into our enterprises. I think 25 billion are going to be here by 2020 according to the IDC analyst. They're being incorporated into houses, into businesses, into government organizations, and security people are not actually looking at this as it relates to their infrastructure. That's a major concern because only about 10 percent of them, from some studies, have shown they have security baked into them.

Additional Resources

- ICI Information Security Resource Center
- ICI Viewpoints: Cybersecurity at Work: The Benefits of Information Sharing Networks
- ICI Viewpoints: Cybersecurity at Work: Exercise Is Important
- ICI Viewpoints: Cybersecurity at Work: Incident Response Plans and What They Entail
- ICI Viewpoints: Cybersecurity at Work: Creating Passwords That Are More Secure
- Video Highlights: 2016 ICI Global Cybersecurity Forum
- Video: With Cyberthreats, Preparation and a Quick Response Are Key