The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

ICI VIEWPOINTS

June 16, 2016

Cybersecurity at Work: The Benefits of Information Sharing Networks

Part of a monthly series of ICI Viewpoints *covering cybersecurity issues.*

In the last installment of this blog series, we wrote about the need for training—specifically, cyber tabletop exercises. Training is important and a well-trained team will undoubtedly respond to a threat in a more precise and effective way than an untrained team. But an important question remains: what will they respond to? It is crucial that a firm understand who is targeting them, why they are being targeted, and what is being targeted. Only by understanding the threat landscape can a firm's defense be more effective and efficient.

For example, information security teams should ask such questions as: are attackers defeating our security or bypassing it? If they are bypassing it, are they using electronic spear phishing or human spear phishing? If it is human spear phishing, then how you train employees about this risk will be very different than how you'll train them to defend against electronic spear phishing.

Knowing who is attacking you and how they are doing it (the attack vector) will help your firm direct its limited human and financial resources to effectively address these risks. So, where and how does a firm acquire this information? Part of the answer can be found in information sharing networks—but there are many different types.

A Foundation of Trust

If you follow cybersecurity events you may have heard calls for businesses to better share cyber-related information within a sector, across sectors, and with government. This, however, raises many questions, including who should share information, what should be shared, when it should be shared, and what should be done with the information. Where is a firm to start? I would argue that the foundation of any information sharing network is trust, and that a great place to begin is within your own industry, with peers at other firms.

This is why ICI and ICI Global have committees specifically designed to bring information security professionals together to share information and to get to know—and, more important—trust each other. Such meetings, held on a regular basis, build trust and an expectation of collaboration in reducing cybersecurity risks.

There are a variety of formal information sharing networks designed to accept incident, threat, and vulnerability data and distribute information about mitigation tactics, threat alerts, and sound security practices, including the Financial Services Information Sharing and Analysis Center and Soltra Edge. The former provides subscribers with online tools to

submit threat data and pushes out alerts, while the latter offers a machine-to-machine readable feed of threat and security data that can be shared in near real time.

Converting Information into Action

The key for any organization, however, is being able to convert the information offered by such groups into a meaningful action. Some firms, particularly smaller investment companies, may struggle with this step. Combatting cyber risk is enhanced by interpersonal relationships—be it within an industry, across industries, or with government agencies (such as law enforcement). With this in mind, I have three suggestions:

- First, if you haven't already, join ICI's Chief Information Security Officer Advisory Committee and/or ICI Global's Information Security Officer Committee to see first-hand the commitment, trust, and cooperation among peers to combat cyber threats.
- Second, to build regional relationships, join the FBI's InfraGard network, a public/private hub that enables users to share information face-to-face and via a web portal.
- Lastly, become part of an information exchange such as U.S. CERT, which enables participants to submit and view threat data via a web portal.

Cyber*in*security is a risk we all face together. Each of us only sees a small piece of this risk. By coming together in a cooperative and collaborative spirit, we can get a better picture of the entire puzzle—as well as some solutions. Don't be like the kid in high school who was always out of the loop on everything and then wondered why he didn't know about the "big party." It's not about being cool—but about being connected.

Do you know what is being said about you? Keep an eye out for the next post in this series, which will examine this question and why it matters.

Additional Resources:

Information Security Resource Center

Other Posts in This Series:

- Cybersecurity at Work: Creating Passwords That Are More Secure
- Cybersecurity at Work: Incident Response Plans and What They Entail
- Cybersecurity at Work: Exercise Is Important
- Cybersecurity at Work: The Benefits of Information Sharing Networks
- Cybersecurity at Work: The Risks of Information Sharing
- Cybersecurity at Work: Keeping Secure When Away from the Office
- Cybersecurity at Work: I Know What You Know!
- Cybersecurity at Work: To Confront Evolving Threats, Flexibility Is Key