The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

ICI VIEWPOINTS

June 5, 2018

For Good Cybersecurity, Keep Your Eye on the Basics, Says Fidelity's Chad Renfro

The computer breaches and hacks that make headlines are typically massive and complicated, and are sometimes even driven by nation-states pursuing cyber-dominance on a global basis. This can lead to the belief that information security solutions must be similarly complex—but good cybersecurity doesn't have to be complicated or expensive, Chad Renfro, head of enterprise cybersecurity at Fidelity Investments, told a capacity audience at ICI's recent General Membership Meeting. Instead, he said, companies that make "strategic, optimized investments in cybersecurity" and that focus on the fundamentals—applying software patches, controlling access to systems, monitoring activity—can drastically reduce the amount of risk facing their firm.

Managing the Cyber Portfolio

In a fast-moving, entertaining exploration of his approach to information security, Renfro talked about his two decades of experience, the more than 500 cyber-incident investigations he's led, and what he's learned during that time. For example, he said that working at Fidelity has taught him to manage information security in the same way that investment managers approach their portfolios. "Every morning, we look at a set of research associated with movements and trends related to the criminal elements that are out there," he explained. The team also follows a framework that enables them to break large tasks into small, more easily managed components.

His team begins by focusing on two things: the intentions and the capabilities of their adversaries, which he separates into four basic groups: cyber-criminals, insider threats, "hacktivists," and state actors. Of these, he said, the first is by far the most important, accounting for three-quarters of his team's time and effort.

The intention of cyber-criminals, Renfro said, is simple: they want money. They're focused on liquidity and they innovate quickly, which can make it particularly difficult to protect personal or organizational information from them—especially if an organization is only reacting to, rather than anticipating, threats.

The solutions in this space involve an unrelenting focus on the basics, as well as the human variables in the equation, Renfro said. For example, he explained, more than 90 percent of breaches of cloud-based systems were due to poorly configured storage setups, while roughly 80 percent of the more than 1,000 reported breaches last year could be traced back to people not applying software patches in a timely fashion.

Because of the “security and product explosion” that individuals and firms are facing—the average PC today has 74 applications on it, he said—it’s essential to follow good practices in configuring and updating systems. “At Fidelity, we have more than 186 security controls just dedicated to the protection of the enterprise,” he revealed. “And those aren’t because we’re unique or big—it’s because the product diversity that we have mandates that.

“If we want to get things right,” he continued, “we’ve got to make sure we’re turning on and working all of those security controls.”

“Collect It and Protect It”

The second threat Renfro mentioned, insider threats, come from two sources: malicious insiders who willingly steal company secrets or property, and insiders who unintentionally cause damage, such as employees who lose laptops or phones containing sensitive data, or those who unknowingly provide bad actors with access to a company network by clicking on, say, a link in a phishing email.

The capabilities of such threats range from very high (developers who believe that the code they create on behalf of the company is actually theirs, and steal it) to very low. The solution, he said, is to “collect it and protect it.” This translates, he explained, to a “focus on attribution,” where every keystroke in an organization needs to be logged, characterized, and associated to an individual.

In addition, Renfro keeps an eye on certain events where insiders can present more of a threat. Because “insiders leaving a company are 71 percent more likely to steal information than those who are not,” organizations should create a program monitoring events such as reductions in force or mergers and acquisitions. In addition, he said, IT needs to work closely with other departments throughout the firm, such as Human Resources, to coordinate efforts around employee departures.

Hacktivists, the third threat, have low capabilities, but are ideologically motivated—which can make them unusually persistent in their efforts, Renfro told the audience. “Anything that has sides on it, you’re going to see these groups focused in on,” he explained, adding that fund managers should be aware that an investment involving any amount of controversy could make them a potential target.

The fourth and final threat he examined was nation-states. Though he said they’re the least-likely threat that the fund industry will face, Renfro did warn the audience that the capabilities of state actors are growing quickly, and that there is a real risk of breaches revealing embarrassing details about staff, or of companies getting caught up in ransomware requests. Attention to the basics should be a firm’s first line of defense in this area, he counseled.

Building Upon a Solid Framework

For all of his focus on the basics, Renfro acknowledged that information security can indeed be a complex undertaking—which is why he’s a firm believer in choosing a framework as a structure for cybersecurity. His framework of choice is the National Institute of Standards and Technology (NIST) Cybersecurity Framework, which is organized in five parts:

1. Identify threats
2. Develop protections
3. Monitor if those protections are being breached
4. Know how to respond to a breach

5. Know how to recover from a breach

Under these five areas, NIST has laid out a total of 23 capabilities—specific areas that corporations must manage to stay on top of cybersecurity threats. “Lots of corporations are fighting the last battle,” Renfro said. “You need to be able to anticipate threats—and this framework provides a good model.”

When Renfro talks to boards of directors, however, he doesn’t talk in terms of frameworks; instead, he boils his work down to three basic areas, with corresponding questions:

1. Customer protection—how do I make sure that I can secure customer transactions?
2. Insider threat—once you trust me with data, how do I protect it?
3. External defense—how do I detect and prevent attacks from the outside on a comprehensive basis?

Asked by GMM Chair Stuart Parker, president and CEO of PGIM Investments, about the most important things that people can do to protect themselves from cyber threats, Renfro summed things up with a analogy.

“It’s like a lot of complex topics—you have to reduce your understanding and response to a few key things,” he explained. “For example, in medicine—which is one of the most complex topics on the planet—your provider is always going to come back to some key things: ‘don’t smoke, exercise, eat well, get enough sleep.’ Cyber is the same way. You need to do five basic things: patch your systems, write your code securely, encrypt your data, monitor your systems, and test your employees for phishing.

“This is not a game,” he concluded. “There are major ramifications with these breaches, so you need to avoid them.”

Copyright © by the Investment Company Institute. All rights reserved. Information may be abridged and therefore incomplete. Communications from the Institute do not constitute, and should not be considered a substitute for, legal advice.