Focus on Funds: Changing Technology Brings New Cybersecurity Demands

Focus on Funds

Changing Technology Brings New Cybersecurity Demands

Fund operations teams face a number of new challenges, including cloud computing and the need to manage third-party vendors. In the March 24, 2017, edition of *Focus on Funds*, cybersecurity expert John Pescatore, director of the SANS Institute, details the latest trends—and best responses.

Transcript

Stephanie Ortbals-Tibbs, media relations director, ICI: In the fund industry, third-party vendors are critically important and that's exactly why their cybersecurity is equally important. At ICI's recent cybersecurity conference, I got some advice on how to manage it.

John Pescatore, director, the SANS Institute: Well, I think that one thing that has changed in the use of third parties over the recent years is the speed we need to do it. So it's one thing to say that we're going to make sure all of our suppliers are secure and our business partners are secure, and we'll call you back in six months. And the answer today is, "No, we need to do this by Friday."

So, the speed has changed quite a bit. And the way security groups, or audit teams, need to be able to say, "We've looked at the risk, we've minimized the risk, and there is some left, we hand it off to you, the business side," has to change as well. Not just to be able to more quickly say, "It's risky, over to you," but be able to quickly assess the risk and come up with ways to mitigate the risk, so that the business unit or even the customer can connect, and business can happen at the speed it needs to happen.

Ortbals-Tibbs: So John, you're talking about moving at warp speed and then into the mix, too, we have to bring the issue too of cloud computing, which is ubiquitous these days and a real factor.

Pescatore: Sure. Cloud computing to me is sort of an aspect of a phenomenon that we've been seeing for a while now. I call it "choose your own IT." Remember, at the beginning, we called it, "Bring your own device"—when the CEO or the head of finance wanted to use an iPhone, or wanted to bring his own laptop or his own iPhone. What's really happening is that people at home—consumers—are using new technology very rapidly and finding it valuable at home, and then wanting to use it at work for value.

The cloud is the same thing. People at home started using Dropbox to share pictures with people or, later, on Instagram, or other

cloud services, they started using email in the cloud at home and found out, “Wow, I can now check my email across a wide range of devices.” Those same people work at our companies, and when they have a new business need, they say, “Why don’t we use the cloud to do that?” And that’s happening much more quickly than putting together a requirements document, getting a team together, requesting resources, and then in a year and a half, we’ll roll out a business system.

So business needs to be able to incorporate things like that, and not say, “No, we have to do it the old way of doing things.” And for security, it means a lot more moving parts to check—it’s not just what’s running in our data center, it’s some in our data center, some out of the cloud, some here, some there, and on devices we didn’t choose. And so the ways that we check third parties for security, the way we evaluate different pieces, also have to change and be able to do what I call “fast-tracking”—so we have the full security thing we go through, but we also have some way we can make a quick assessment and allow business to move on, while we continue to monitor and work to get the security level increased, but not try to stop business at the beginning.

Ortbals-Tibbs: You also shared a lot of perspective about the difference between compliance and security and how to make sure that you’re not just checking boxes.

Pescatore: Yes—especially in finance, it’s a regulated environment, there’s going to auditors, there’s going to be regulations we have to prove that we comply with. But those regulations exist to persuade businesses to protect their customers. They’re not there to satisfy the government. They’re there because someone in the government said that this is the way to protect customers. So what we always need to do in business is, first, do what we need to do to protect the customers and protect the business, and then demonstrate compliance to the auditors.

So the bad thing about compliance is, if the strategy is, how do we more quickly and cheaply achieve compliance, huge gaping holes are left. Every breach you’ve read about in the news? Those companies were compliant with the payment-card industry data-security standards. They were compliant, but they weren’t secure. If you go the other way around and you get secure first, you’re almost automatically compliant. And if you’re not compliant, it’s usually a matter of documentation, not actual security levels. So really, avoiding the compliance trap means, get secure first, then demonstrate to the authorities [that] your version of security meets their requirements.

Additional Resources

- Highlights from ICI’s 2016 Cybersecurity Forum
- ICI Information Security Resource Center
- *ICI Viewpoints* Series: Cybersecurity at Work
- *Focus on Funds*: How Can You Benchmark a Cybersecurity Response Plan?