RIAs Make Great Targets for Hackers, Cybersecurity Cop Says

May 1, 2019

After more than 30 years of managing technology in high-level positions in a variety of industries, Wes Stillman founded Lenexa, Kan.-based RightSize Solutions in 2002. It was the first provider of outsourced technology management and cloud-based cybersecurity solutions for registered financial advisors. In 2018 it launched the RightSize Shield, which it calls "the most comprehensive, flexible and completely compliant cybersecurity solution for RIAs."

Stillman believes that a "smart" technology infrastructure goes beyond protection against cyberattacks. It can improve efficiency, serve as a platform for growth and, ultimately, increase a firm's valuation, he said.

He recently spoke to Financial Advisor about the growing cybersecurity threats financial advisors face and what they can do about them.

How did you come to focus your business on financial advisors?

When I got the opportunity to start RightSize Solutions it was very obvious to me that most of the IT providers out there were great at IT but were trying to provide IT to all companies. You can't do cybersecurity as one size fits all. It has to be built around how you work, how you work with your clients and what your clients are going to accept from a security standpoint.

Are there specific threats that RIAs face?

RIAs make great targets for the bad guys out there. Most of them are small organizations, up to as much as 30 to 40 people. And they deal with a lot of money, from a few hundred million dollars to a few billion under management. Over the past year it has become more obvious how vulnerable they are. The SEC has really put a major focus on it, along with the states. In 2015, the SEC started talking about guidelines for cybersecurity. Since then it has moved from not really understanding what needs to be in place for RIAs to being well educated about cybersecurity. We've seen the SEC exam go from four to five questions about cybersecurity policies to more than 40 very detailed questions. So there's no doubt that there is a need for these firms to really engage with someone who understands what the needs are and can help them focus on that.

Do RIAs take cybersecurity seriously?

We hear all the time from RIAs, "I know I need to do something, but I don't know where to start." The SEC's focus is on enforcement; it doesn't help you create a policy on what you should be doing. Our job is to help advisors not only understand what should be in place, but actually make that happen for them. Most RIAs today do have a cybersecurity policy, but it's

usually created through their compliance department. For example, they may have a policy that you're only supposed to get email on your personal phone if it's encrypted. That's a good component to the policy. But they have no way of knowing if everyone in their company is complying with that, and no way of enforcing the policy.

Instead of just reporting on what is out of compliance, we want to make sure that their policies are being adhered to. It's a proactive approach as opposed to a reactive one. We do all the monitoring and reporting on the back end of things, which is important, but once we have that policy in place, we enforce those policies with technology. We work as part of your team—with your compliance group, your operations group. Cybersecurity is not something you can just buy. It's a combination of awareness, training and enforcement, and it's ever evolving.