A third-party cyber attack is your firm's problem

November 21, 2017

Recent high-profile cyberattacks underscore the importance of tracking how and where client data is used, transferred and stored by third party vendors to RIAs. The reality is, "the cloud" is not – and never was – a cybersecurity solution.
RIAs are responsible for telling clients when a vendor is hacked and their data may be at risk. This means firm principals must take a far greater interest in ongoing cybersecurity management than they probably ever wanted. It's not an enviable position to be in, but passivity and ignorance on these issues puts the firm at much greater risks of problems down the road.

RIAs may not ever be able to guarantee the absolute security of client information and assets, but they are not absolved from putting forth their best effort to protect them. Firm owners need to understand the bigger picture around how and where the outsourced cloud-based solutions they have chosen are storing and protecting their clients' data.

VENDOR BREACH

Vendor breaches are vendor issues, right?

Wrong. RIA principals must consider how their responsibility to act in clients' best interests

translates to data and personal information protection.

The checks and balances that advisers employ to run their firms and manage client assets and risk should extend to vendor selection and cybersecurity. This means that before a breach happens, RIAs should be doing due diligence on their vendors to ensure that their cybersecurity protocols fit into the firm's business processes.

(More: Technology issues test RIAs and custodians.)

Choosing common technology vendors or bigger brands does not obfuscate the RIA's responsibility to clients. Just because the vendor is big does not free the RIA from having to understand how they handle their data – i.e., does the vendor use third parties, and if so, how and for what? How do they handle data encryption? Who manages their servers?
And a new crop of technologies in the RIA space means that the best-known brands may not offer the best solutions for some firms. When considering newer entrants to the space, it is critical that firms conduct a thorough cybersecurity vetting process.

Regardless of whether it's an established brand or new provider, advisers have an obligation to their clients to understand how their data is being managed and to take action if a breach happens.

CLIENT DATA
Here's a key question: "Where is my client data?

Suppose a RIA uses a third party for its CRM or for portfolio management. The vendor uses a global computing system, it could be any provider, such as Amazon Web Services (AWS), Microsoft Azure, Google Cloud or another. Now let's say there is a data breach at one of the data centers around the world for this provider. Is the RIA's client data at risk?

While there may be no way to know right away whether client data was compromised, take a step back from for a moment. When choosing the CRM vendor, did the RIA ask which global cloud provider the vendor used? Did the RIA ask where – literally, what country or countries – their client data was being stored?

(More: Someone tried to hack my Social Security account.)

If the RIA does not know where the data is being stored, the firm might not even know that its data was or could have been breached. Firms need to ask their vendors specific questions about where their data is being stored. They also need to ask about the notification process in the event of a breach, particularly if data is going overseas.

Most advisers would probably admit that they have assumed "the cloud" as a mysterious place where their client data and firm information are safe and secure by default. This needs to change. The worst thing an RIA can do is to not ask questions of their vendors. Instead,

RIAs need to probe their vendors on their own cybersecurity protocols so that in the event of an issue, they can communicate with clients with some assurances.

Wes Stillman is the president of RightSize Solutions.

Related Topics: Cyber Attacks