Pensions&Investments

Smaller plans face a bigger burden for cybersecurity

BY MARGARIDA CORREIA · APRIL 15, 2019

Michael Francis said plan sponsors should ask record keepers about their security measures | BRETT KRAMER

Budgets not big enough for specialized staff, so plans rely on advisers

Cyberthefts from 401(k) plans are always distressing, but when they occur in smaller plans, the loss can be especially painful.

Take Michael Francis' $100 million plan sponsor client. Earlier this year, a cyberthief posing as one of the plan's participants managed to trick the company and the record keeper into sending him $35,000.

"Incurring a $35,000 unexpected cost would not be within this organization's budget for retirement plan incidentals," said Mr. Francis, president and chief investment officer of Francis Investment Counsel LLC, a registered investment adviser in Brookfield, Wis.

The client, whose name Mr. Francis declined to disclose, was one of several small and midsize plan sponsors that have been recent victims of cybercriminals or targets of attempted attacks, he said.

"We started hearing story after story after story," Mr. Francis said. "We spent most of the first quarter having lengthy conversations with all our clients about the sharp increase in attempted cyberthefts from 401(k) plans," he said.

Cybersecurity threats impact plans of all sizes, but smaller plans face even bigger challenges given their lack of resources. Unlike large employers, small companies can't afford to hire a chief security officer or have staff dedicated to cybersecurity issues. As a result, many small and midsize employers are relying more on their retirement plan advisers for guidance, according to industry observers.

"Small- and medium-size employers don't have anyone to turn to in their organization, so they're more dependent on help from other sources," said Tim Rouse, Simsbury, Conn.-based executive director of the Spark Institute Inc., a retirement industry trade association.

The challenge is especially acute for advisers who work with plan sponsors part time, according to Mr. Francis. Advisers serving the small plan market are more likely not to be 100% focused on defined contribution plans, concentrating instead on wealth management business, he said.

"It's really hard to keep on top of all this stuff because there's so many other things that they're worried about," Mr. Francis said.

Preventive measures

Mr. Francis, whose business is entirely focused on plan sponsors, regularly coaches clients on what they can do to avert cybertheft. He urges them to contact their record keepers about what they are doing to keep cyberrisks at bay and to inquire about advanced security measures, such as biometric/voice recognition software. He especially advises them to understand the service agreements they have with their record keepers and to ask about their policies for account reimbursement.

Plan sponsors should understand under what circumstances the record keeper would not make a participant whole following a successful breach, said Mr. Francis, whose firm has 70 qualified plan sponsor clients and oversees $8.3 billion in assets under administration.

In the case of the 401(k) participant who had $35,000 fraudulently taken from her account, the employer and the record keeper agreed to split the cost to make the victim whole. But it was contentious, Mr. Francis said, "with the record keeper pointing at the employer and the employer pointing at the record keeper" as the party liable for the loss.

Andre Huaman, a partner with registered investment adviser firm Three Bell Capital in Los Altos, Calif., said he also has seen a substantial increase over the past year in the number of clients and prospects asking about cybersecurity. "They are leaning on us as their advocates to complete proper diligence related to the record keeper and their cybersecurity protocols," he said.

Mr. Huaman said his company vets record keepers for its clients, a process that usually takes a year. The firm looks at the provider's long-term growth of assets and clients, cybersecurity protocols, management and leadership team, relationship managers and their tenure in the industry, among other factors.

"Most of the large record keepers are dealing with thousands of cybersecurity threats per day, so it is vital that our team help our plan sponsors complete diligence on the cybersecurity capabilities of these providers," Mr. Huaman said.

Top concern

Pat McGowan, manager of benefits outsourcing company AlphaStaff Inc.'s multiple-employer 401(k) plan, said that the "humongous breaches" at Equifax Inc. and other organizations has pushed cybersecurity to the top of the list of concerns for the 241 small employers in the $100 million plan. While the plan has not had any successful breach attempts, he suspects that multiple-employer plans might be more vulnerable to cyber issues due to having "more moving parts."

"We do have a lot of moving parts with regard to the interchange of employers that come onto our platform," Mr. McGowan said. "In the one-company XYZ world, they have just one set of rules that applies to everybody."

Amid heightened concerns, record keepers are stepping up efforts to educate advisers. Fidelity Investments, for example, held all-day adviser events last summer in nine cities across the U.S. in which cybersecurity was a featured topic. Empower Retirement, likewise, has been ramping up efforts since 2014 to communicate with the 30,000 advisers on its platform about cybersecurity issues. In a tech guide distributed to advisers, the firm provided tips on what advisers should look for in their clients' record keepers, including a list of questions to ask.

"The intent behind the guide is to try to make a distinction between what's really important for a record keeper … vs. those things that are secondary and tertiary," said Doug Peterson, Denver-based vice president of information systems for Great-West Life & Annuity Insurance Co., Empower's parent company.

Mr. Peterson chairs the Spark Institute's Data Security Oversight Board, which developed 16 broad categories of data security reporting by which independent third-party auditors can assess and grade a record keeper's cybersecurity systems. So far, seven record keepers have tapped accounting firms to audit their cybercapabilities using the Spark Institute's reporting road map, according to Mr. Rouse. The auditors will identify the controls that are in place for each of the 16 categories so advisers can "begin to score each company" and "do an apples-to-apples comparison," Mr. Rouse said.

"It allows you to be better educated and ask more pointed questions to get to a higher level of comfort that the vendor that you're working with is meeting your needs," he said.

CONTACT MARGARIDA CORREIA AT MCORREIA@PIONLINE.COM

Original Story Link: https://www.pionline.com/article/20190415/PRINT/190419943/smaller-plans-face-a-bigger-burden-for-cybersecurity