Pensions&Investments

Gaps remain in perception of cyber threats

Execs confident providers' practices are sound; professionals say otherwise

By: Robert Steyer
Published: August 24, 2015

International Foundation of Employee Benefit Plans' Julie Stich: 'Sponsors might not be as aware as they should be. (They) should be more concerned."

Efforts by defined contribution and other employee benefit plans to improve cybersecurity appear to reflect a paraphrase from former Defense Secretary Donald Rumsfeld: They don't know what they don't know.

Although a recent survey showed a majority of DC plan executives expressed confidence in their service providers' cybersecurity policies and practices, cybersecurity specialists and ERISA attorneys say many benefits plans still need more work to achieve greater protection.

"The mantra of cybersecurity professionals is that there are two types of people," said Matthew E. Jackson, a New York-based senior vice president for Segal Select Insurance Services Inc., an insurance brokerage and subsidiary of The Segal Group Inc. "Those that know they have been hacked and those that don't know they have been hacked."

Experts and attorneys say benefit-plan executives are taking steps to improve cybersecurity, such as demanding more detailed answers from providers in RFPs and conducting more stringent internal reviews of plan policies. However, they warn that the industry as a whole isn't treating such protection as a top priority.

"This is an issue that has gotten very little attention" among DC plans, said Jeffrey Capwell, a Charlotte, N.C.-based partner at McGuireWoods LLP, and head of the law firm's employee benefits and executive compensation practice.

"Wait until there's an Anthem-like security breach in the retirement context," said Mr. Capwell, referring to the hacking of data at Anthem Inc., the Indianapolis-based health benefits company, that exposed information on as many as 80 million people. "Then, there will be a greater focus."

A May 2015 report by the Ponemon Institute, Traverse City, Mich., said the "average total organizational cost" of data breaches reached $6.53 million, based on a review of 62 U.S. companies that experienced breaches primarily in 2014 but also in 2015.

The institute, whose data-breach work is sponsored by IBM, has conducted annual surveys for 10 years. The average cost was $5.85 million in last year's report. Ponemon's annual surveys examine incidents involving 100,000 or fewer compromised records.

Not much research

Research on DC plan executives' attitudes and actions regarding cybersecurity is meager. In a recent broad survey of 398 DC plan practices, Deloitte Consulting LLP asked several questions about cybersecurity, finding that:

nFifty-nine percent of DC plan executives said they were very confident in their providers' cybersecurity practices while another 30% said they were somewhat confident.

nNinety-three percent said their data hadn't been compromised. Four percent said their data had been compromised within the last year (for plans with more than 10,000 employees, the rate was 9%.) Among the broader group, 2% said their data had been compromised one to five years ago; and 1% said their data had been compromised more than five years ago.

nSeventeen percent have never reviewed providers' cybersecurity policy and procedures, while 3% reviewed them more than five years ago. Fifty-five percent conducted a review within the past year, while 25% reviewed it one to five years ago.

Some cybersecurity experts said they were skeptical of some Deloitte findings.

“It's been my experience that plans don't follow through on monitoring” of providers' cybersecurity practices, said Mr. Capwell, adding there's more to ensuring protection than issuing an RFP. “Sponsors need to follow through contractually with reporting obligations,” he said. “You need more rigor in your contract with your provider.”

Mr. Jackson added he has seen an increase in requests by DC plans and other benefits plans for more cybersecurity information in RFPs, plus stronger wording in existing contracts and a greater interest in insurance.

“Two or three years ago, when we talked to sponsors, there was not a lot of interest” in cybersecurity insurance, he said. However, in the past six months, there has been an increase in the number of benefits plans asking about and buying such insurance.

Mr. Jackson couldn't quantify the amounts, adding the overall percentage is still small.

Greater concern

Another survey of a broader group of 179 benefits plan executives found cyberattacks and internal security data security breaches were bigger concerns than workplace violence, terror attacks or disease, said Julie Stich, research director of the International Foundation of Employee Benefit Plans, Brookfield, Wis., whose organization published the survey in March.

Despite plan executives' concerns, “I do think sponsors might not be as aware (of cybersecurity problems) as they should be,” said Ms. Stich. “I think sponsors should be more concerned.”

Among the sources of trouble: employees who take a laptop home and then lose it; computer system failures; inadequate password protection; and failure to destroy obsolete information.

“The danger is one of complacency,” said Mark Nicholson, principal for Deloitte Cyber Risk Services, noting that the investment management sector — benefits plans, mutual fund companies, hedge funds and private equity firms — is “relatively immature when it comes to cybersecurity.”

They haven't devoted a large amount of money to cybersecurity, in part because “it hasn't been a proven risk issue for them,” he added. “There is a prevailing perspective that investment managers aren't a target” of hackers.

Mr. Nicholson's offers this advice to clients: Be secure in your technology; be vigilant in monitoring internal and provider cybersecurity policies and practices; and be resilient by having a response plan in place and conducting cybersecurity breach simulations.

Patchwork of laws

Another cybersecurity challenge is the uncertainty caused by a patchwork of laws and regulations — both state and federal — governing liability and responsibility.

Part of the problem is the Labor Department "has been relatively quiet on this," said Stephen P. Wilkes, of counsel to The Wagner Law Group in San Francisco. "There is a lack of specific guidance under ERISA."

Mr. Wilkes said the department needs to answer many cybersecurity questions. For example: Is plan data considered a plan asset for ERISA purposes? Is cybersecurity a fiduciary act?

Mr. Wilkes said the DOL should conduct a "gap analysis" to study where laws and regulations are inconsistent, contradictory and/or silent on cybersecurity and retirement plans. At the very least, he added, the DOL should issue guidance and clarification for sponsors and providers outlining industry best practices.

Absent DOL guidance, many sponsors have been adopting best practices regarding retention of data, requiring more detailed information from providers and educating employees. "Best practices demand that sponsors treat cybersecurity as a fiduciary matter even if the laws are unclear," Mr. Wilkes said.

Original Story Link: http://www.pionline.com/article/20150824/PRINT/308249975/gaps-remain-in-perception-of-cyber-threats-execs-confident-providers-practices-are-sound-professionals-say-otherwise