Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

4 Tips For Handling Retirement Plans' Cybersecurity Risks

By **Emily Brill**

Law360 (June 7, 2019, 9:34 PM EDT) -- Employers who want to protect their retirement plan from a data breach — and limit their liability if one occurs — should evaluate and address sources of risk, analyze their contracts with companies that service the plan and ensure any cybersecurity measures instated at the company cover the plan as well, attorneys said.

Cybersecurity issues have been a hot topic in the benefits space for about a year, attorneys say, gaining momentum after a ransomware attack at the UFCW Local 655 Food Employers Joint Pension Plan and amid a national conversation about corporate data security.

Though courts have not weighed in on whether the Employee Retirement Income Security Act obligates plan fiduciaries to monitor cybersecurity risks, attorneys say they wouldn't be surprised if judges ruled that it does.

"It's not difficult to see how the failure to take adequate precautions could be seen as a breach of fiduciary duty," said Matthew Hawes, a benefits partner at Morgan Lewis & Bockius LLP. "I don't want to say there absolutely is a fiduciary obligation until the courts tell me so, but on the other hand, I don't want to see our retirement plans at the wrong end of a lawsuit."

In the absence of court guidance, a 15-member group of government-appointed retirement experts called the ERISA Advisory Council has asked the U.S. Department of Labor to explain how plans should respond to cybersecurity risks.

Private actors have also stepped in, with a money managers' lobby called the SPARK Institute developing standards for plan recordkeepers to share cybersecurity capabilities with plan sponsors, and the University of Pennsylvania producing a white paper called "Benefit Plan Cybersecurity Considerations: A Recordkeeper and Plan Perspective" last year.

"It was about a year ago when people started talking about [cybersecurity issues in employee retirement plans] with more vigor and specificity. I remember more papers and suggestions about it and, really, more questions: What are the standards, or what ought they be?" said Mark E. Schreiber, the leader of McDermott Will & Emery LLP's global privacy and cybersecurity practice, who also worked as an employment litigator for 25 years.

In the absence of case law and government guidance, Schreiber said he has found "not a lot of good

answers, or at least determinative ones" on what plans should do about cybersecurity, though he praised the efforts of the ERISA Advisory Council, SPARK Institute and University of Pennsylvania.

Hawes said it's up to retirement plans themselves to figure out how to take action to evaluate data risks and help protect their workers' data.

If they don't, they could be hit with a hefty bill if a cyberattack occurs, he said. IBM estimated last year that data breaches cost companies $148 per stolen record, with the costs sourced to clean-up activities like credit monitoring, notices and investigations into what happened.

"There's also the overarching fiduciary duty to act in the best interest of participants," Hawes added. "It's common sense to protect this data, but then there's the overlay of fiduciary obligations."

Law360 asked Hawes and Schreiber, who both advise companies on cybersecurity obligations, to list their best practices for benefit plan managers looking to protect workers' data. Here are four tips they offered.

Evaluate and Address the Sources of Risk

First, figure out who has access to workers' data, Hawes said. This can include human resources professionals, plan trustees and third-party vendors that contract with the plan.

"Once you can identify the sources of the risk, then you can start to look at steps that can be taken to mitigate that risk," Hawes said.

Schreiber recommended bringing in a third-party vendor to do a cyber risk assessment, which identifies vulnerabilities in a company's network.

He also recommended having an attorney supervise the assessment so it is protected by attorney-client privilege.

"Risk assessments turn up all kinds of material," he said.

Extend Company's Cybersecurity Measures to its Retirement Plan

In an age when huge data breaches have hit Marriott, Equifax and Yahoo, corporations are on high alert about their susceptibility to such an event.

Because of this, many have implemented cybersecurity measures. Hawes says employers should make sure they're extending these measures to the employee retirement plan, whose plan managers may be making some of the same moves.

"A lot can be gained by coordinating those efforts," Hawes said.

Ensure Vendors are Using Cybersecurity Measures

Employers should familiarize themselves with third-party vendors' cybersecurity efforts before hiring them to work with the plan.

“Make sure you’re addressing data security as part of the [request for proposals] process,” Hawes said. “Make that part of the selection process for vendors.”

After choosing a vendor, employers should ensure their contract with the company addresses data security obligations, being clear about who’s liable for what if a data breach occurs, Schreiber said.

Once the contract is signed and the vendor begins working with the plan, employers should check in from time to time to make sure the company is still delivering on its cybersecurity promises.

“Make sure you engage with the vendor to get representations from them that they’re providing the appropriate level of security, and make sure they’re providing reports,” Hawes said. “Having a regular report from the vendor back to the retirement plan fiduciaries is an important step.”

Get Insurance

Because data breaches can cost a lot of money, attorneys often advise companies to buy insurance that will cover them in the event of a cyberattack. Plan managers can look into this as well, Hawes and Schreiber said.

“Take a look at your fiduciary liability policy to make sure it covers data security events, and, if necessary, purchase a rider to make sure you have coverage,” Hawes said.

Schreiber added that so-called cyber liability insurance is becoming “more common and useful,” and it shouldn’t be hard for companies to find.

“There are a number of very good brokers out there that can help you locate the best policy,” he said. “All the major insurance brokerage houses all have cyber insurance advice units.”

--Editing by Emily Kokoll.