Risk for Cyberattacks Heightened as Remote Work Continues | PLANSPONSOR

Amanda Umpierrez

The widespread move to remote work in light of the COVID-19 pandemic means plan sponsors should take a careful look at their cybersecurity measures.

To drive the urgency home, lawsuits alleging cyberfraud negligence have been on the rise—MandMarblestone Group (MMG), Nationwide, Abbott Laboratories, Alight Solutions and Estee Lauder have all faced litigation in the past year.

In the case of *Leventhal v. MandMarblestone Grp. LLC*, plaintiffs said working remotely without a secured network exposed a plan participant's personal information. A cyberhacker allegedly obtained a copy of the participant's withdrawal information, falsified a duplicate and submitted the forged document by hacking into the office administrator's home network, notes Carol Buckmann, founding partner and ERISA [Employee Retirement Income Security Act] attorney at Cohen & Buckmann. The cyberhack resulted in a loss of $400,000 to the participant's account. Nationwide, the service provider to the plan, submitted a counterclaim against the plan sponsor, alleging that MandMarblestone Group had been careless when it came to monitoring its computer/information technology (IT) systems and employment policies while allowing its employees and participants to work remotely.

"Having remote work adds a special challenge," Buckmann adds. "This is an illustration of the danger of not having control over the security of home computers."

Not every hack is done online, however. In the case of Abbott Laboratories and Alight Solutions, where the latter served as recordkeeper to the plan, an imposter allegedly spoke over the phone with a call center representative in order to process account withdrawals. The recordkeeper had failed to follow up with an email confirming the withdrawals, only sending confirmation via snail mail. By the time the participant received the letter, the money was already gone from the account, according to the lawsuit. "Some of these problems could be prevented if people were asked to provide real-time information," Buckmann notes. "Employers have phone numbers on file, email addresses, security questions, etc. There are real-time confirmation points."

But this abundance of participant information, with numerous storage points, can have critical side effects for participants, plan sponsors and service providers. Rob Projansky, a partner in the Employee Benefits group for Proskauer, explains that, aside from a hacker stealing money, there's the drawback that defined contribution (DC) plans have an extensive amount of sensitive employee data shared through multiple channels. This distribution of information faces greater risk as plan professionals and participants access unsecured networks at home without proper security protocols.

Projansky says the personal material includes "Social Security numbers, birthdays, bank accounts, medical information, beneficiary information, etc."

"And the other problem is that benefit plans don't just hold the data themselves," he adds. "They share it with service providers, and that creates numerous points of entry for cybercriminals. The cybercriminal doesn't even need to fool the plan for a breach, it can fool the vendor or the participant, people for whom the plan has a lot less control."

The economic fallout caused by the pandemic also encourages hackers to exploit these openings. The passage of the Coronavirus Aid, Relief and Economic Security (CARES) Act has eased the process of withdrawing assets from a DC plan and removed early withdrawal penalties. Jordan Mamorsky, of counsel at the Wagner Law Group, says he supposes that a portion of increased personal withdrawals from these accounts will be cyberattacks. "This is why it's important for plan sponsors to realize that they are exposed, their participants are exposed, and they need to implement measures to make sure they are adequately protected under the law and under ERISA," he states.

The Cybersecurity and Infrastructure Security Agency (CISA) has released free services and cyber resource hubs, along with telework guidance and resources to assist in combatting cyberattacks, especially in remote work environments. While plan sponsors can find tips and best practices for securing their networks, there is little guidance on what prudence looks like when it comes to protecting participants' cybersecurity. Instead, the Department of Labor (DOL) expects plan administrators to already have security measures in place. "There are a lot of moving parts here, and there is no objective bright line practice that administrators can adhere to," Mamorsky says.

While the DOL offers limited guidance, there are still best practices employers can use to minimize their risk of a cyberattack and any future litigation. Plan sponsors can send cyber tips on working remotely to participants, encourage workers to lock their computers, turn off personal electronic assistants, lock video conferences, hide personal information while on video, secure passwords, stay alert to phishing, and properly store and destroy documents, Projansky says.

Implementing two-factor authentication will also diminish cyberattacks, Buckmann adds. "People are now even thinking about other factors of authentication. They can do voice authentication, where they can match your voice—there's all kinds of technical advancements that can be helpful here," she says.

When selecting a plan provider or partnering with third parties, Mamorsky recommends employers review plan documents and contracts with service providers to ensure they feel comfortable with the provisions of the plan. Employers also should implement a request for proposals (RFP) process that asks how a vendor is committed to data privacy and what their security process entails, Projansky advises.

Additionally, Projansky recommends combing through cyber-liability insurance with the help of an experienced broker and an insurance specialist attorney, who can take a look at the policy and suggest types of coverage that are essential and what to ask for.

It's important to note that cyber insurance has certain key features distinctive from other plan policies, Projansky says. He says plan sponsors should ask if the policy covers data that is in control of independent contractors. Does it cover investigations? Does it cover social engineering? Are there any exclusions for ERISA violations? "People need to hone in on what those policies say to make sure that they have the coverage that they think they do, and the coverage that they want," he says. "It's an investment, but it's a small investment relative to a large risk."