IGNITES
A Financial Times Service

401(k) Firms Form United Front to Thwart Cyber Attacks

By Emile Hallez May 7, 2018

Hackers are increasingly working to access and loot retirement accounts, prompting an industry group to create an information-sharing coalition that allows recordkeepers to anonymously report cyber attacks to peers.

Late last month, the Spark Institute announced a collaboration with FS-ISAC, the public-private partnership that facilitates the sharing of cyber-threat intelligence between thousands of financial services companies. The two organizations formed the Retirement Industry Council, which functions as a group within FS-ISAC, or the Financial Services Information Sharing and Analysis Center.

So far, 21 U.S. firms have signed up to participate, and several Canadian retirement services companies have also expressed interest, according to Spark.

Formed in 1999, FS-ISAC allows banks, fund providers and other types of financial services firms to share information, but until now, there has not been a channel specific to the retirement plan business. That has made cyber-attack communication difficult for 401(k) recordkeepers, says Doug Peterson, head of information security at Empower Retirement and chair of Spark's Data Security Oversight Board.

"The problem that exists for us, as recordkeepers, [is that] it's like drinking from a firehose," Peterson says. "There is an enormous amount of information that gets put in by these companies.... It's just too much."

And with a daily barrage of phishing attacks, both plan recordkeepers and individual participants are constantly at risk, those who work in the industry say.

The bulk sale of personally identifying information over the dark web has armed nefarious account hackers with an unfathomable amount of data to exploit.

In response, the industry has implemented multi-factor authentication as a necessary step for users to log into their accounts. Before gaining access, users must enter confirmation codes sent to their phones or e-mail accounts, for example.

But even then, hackers have found a way through the safeguards.

Recently, malware has been included in a solitaire game for mobile devices, for example. That malware, called "marcher," quietly takes control of the device, gaining access to numerous accounts and enabling third parties to see the multi-factor authentication codes sent to the user's phones, said Rachel Wilson, a former NSA employee who is now head of cyber security at Morgan Stanley.

For willing buyers, the marcher malware has been available for about $60 on the dark Web, Wilson said, speaking last month at the National Association of Plan Advisors 401(k) Conference in Nashville.

Because hackers' methods have become more sophisticated, firms are beginning to add biometric screening to their login process, she said. Morgan Stanley, for example, records profiles of customers' voices for about 30 seconds and later uses that profile to positively identify callers during "natural conversation," she said.

Even if a caller can tell a rep the correct answers to personalized questions, transactions will not be permitted if the voice profile does not match the caller, she said.

"We create a profile of their voice that is as unique as their fingerprint," she said. "Expect to see more and more of this from your firms."

The industry needs to work together and freely share information about the cyber-security threats they face, she said.

"We're on a call literally every morning" with other firms, she said. "We recognize that we are going to rise and fall as an industry" by what they are willing to share.

By being able to share up-to-the-minute information about attacks and phishing schemes, many recordkeepers can implement safeguards quickly, Empower's Peterson says.

But one thing that prevents many firms from openly sharing such information is a lack of anonymity, he says.

"We need to be able to have the ability to share without attribution," he says. "We all have this common enemy.... They're using the same attacks with each of our institutions."

One potentially powerful example would be the sharing of a voice profile of a caller attempting to defraud a client, he says. Technology that will allow all firms to screen calls against a database of voice files associated with such fraud attempts made elsewhere already exists, he says.

The ability to share information safely, such as through FS-ISAC, encourages more firms to report problems or attempted breaches of their systems, says Tom Quinn, head of information security at T. Rowe Price.

"We have seen attacks where it is very broad-based, and it may apply to many firms across financial services," Quinn says. Being aware of the type of attack and approach "allows us to better protect ourselves and manage our response," he says

Phishing has become a prominent risk to clients' accounts, he notes.

"The blending of both work and life — and social media — I think is something for us all to take pause on," he says. Given the refined use of social engineering by hackers, people should consider "how much information is being provided via those channels and whether it is appropriate."

As retirement plan providers have added websites and features for mobile access, they have increased their exposure to malicious attacks, says Erisa lawyer Joan Neri, counsel at Drinker Biddle.

"Cyber attackers are very quickly learning and adapting to the cyber-security practices used by firms," Neri says.

And specific to retirement plan providers working as fiduciaries, there is liability under Erisa, she says. The duties to prudence and loyalty to clients could include measures to ensure that client data is secure, she says.

While freely sharing information about cyber attacks is clearly in the best interest of the industry, there is likely an underreporting of incidents, says Robert Rosenzweig, national cyber risk practice leader at consulting firm Risk Strategies.

Being able to report issues anonymously could be crucial. When firms have been able to control incidents before they have affected customers' accounts, they are less likely to go public with disclosure, in part because they are not required to by any regulations, Rosenzweig says.

Attacks "are happening, but they don't end up in the public domain," he says.

Further, incidents that cause business interruptions appear to be less commonly reported than those in which consumers are directly impacted, he says.

"I'm sure there's some more organic information sharing that's happening among peers, but it's hard to say at what point does the benefit of being a friendly competitor [outweigh] potentially disclosing incidents that could have some financial impact on your organization."