COMPLIANCE | September 28, 2020

PSNC 2020: Retirement Plan Cybersecurity

In light of a lack of guidance from the DOL on how sponsors should protect their plans from cyberattacks, speakers laid out best practices.

Reported by LEE BARNEY

Speaking at the last session of the 2020 PLANSPONSOR National Conference, speakers noted that the Department of Labor (DOL) has not issued guidance for how retirement plan sponsors, acting as Employee Retirement Income Security Act (ERISA) fiduciaries, can best protect their plans from cyberattacks.

"Being logical and practical might now serve us best," Brett Shofner, president of Work Plan Retire, said during the virtual discussion. "For ERISA plans, it is all about protecting participants—not only their money but their data. There are hackers out there, just like out of the TV show, '24,' trying to steal money. Think about internal controls over payroll, HR [human resources] and benefits [workers]. A lot of people have access to sensitive plan data, and all are potential bad actors."

Bart McDonough, CEO and founder, Agio, said, "When we think about the fundamentals of cybersecurity, we think about the 'CIA' framework: confidentiality, integrity and availability of data. When it comes to confidentiality, we ask, 'Do people who should not have my data have access to it? Disruption of the integrity of data is when it is manipulated, and an example of the disruption of data is a ransomware attack, whereby access to your computer is frozen. All three of these are affecting the financial services space."

Unfortunately, McDonough said, "regulations are not clear in ERISA" about plan sponsors' responsibilities when it comes to cybersecurity. "The DOL has talked about securing data, but there isn't a rock solid requirement," he said. However, "depending on the state you are in, there are lots of different regulations that apply."

When it comes to data privacy guidance, for instance, there are 48 different requirements in the 50 states, McDonough said.

Absent this guidance, McDonough said, "You need to have a very good idea about how you are handling sensitive data, and how you will respond in the event of a cyberattack. You need to have an answer to those two questions."

Shofner concurred: "You would think there would be some formal policy, but there is not, and that puts plan sponsors in a difficult position. Knowing that there isn't a formal position, and the DOL hasn't been specific on how plan sponsors can protect themselves, they should be conservative."

Shofner noted that a recent paper by ERISA attorney Marcia Wagner, founder of The Wagner Law Group, said plan sponsors should "take a conservative angle and assume that all of this data falls under the ERISA duty of loyalty and prudence. Should there be a bad actor in payroll, administration, the third-party administrator [TPA], recordkeeper or other service providers, sponsors need a policy on how to respond and evidence of that policy." A good place for sponsors to start is to simply ask their service providers about their cybersecurity defenses and to document these policies in writing, Shofner said.

Complicating matters is the fact that many recordkeepers have overseas offices or call centers, he continued. "The important thing is for plan sponsors to ask these questions," Shofner said. "This is where the plan sponsor has to be specific and drill down on things, like making the service agreement and understand what they are promising to do and hold them to it.

“We are realizing that a lot of plan sponsors are not asking these questions,” Shofner stressed. “In a court of law, one could argue that this is not a prudent position to be in. Asking about their insurance agreements, their standards and their handling of data is critical.”

McDonough said the “CIA” perspective can guide sponsors’ questioning of their service providers. “The first question I would ask of the company is, ‘Who performs a tabletop exercise, and how often do they do that?’”

McDonough went on to explain that a “tabletop exercise” is a “virtual war game where you role-play scenarios.” He also suggested plan sponsors should ask their vendors who owns the data. And while there currently is no regulation on cybersecurity in the United States, he said he believes the nation will eventually adopt something along the lines of the General Data Protection Regulation (GDPR) that exists in Europe.

Shofner suggested that sponsors familiarize themselves with that regulation. “Lawsuits that are coming down on this are fact-specific,” he said. “If you look at these other standards out there that are reasonable, that is a smart move should something go wrong. It shows you are trying to do the right thing, and that can help mitigate damages.”

McDonough said that using GDPR as guidance, sponsors should be asking important questions of their Tier 1 vendors—those that handle personally identifiable information (PII) on their participants—every six months, and their Tier 2 vendors, annually.

He also said it is important to train employees to avoid being hacked because “there are two types of companies: those that have been hacked, and those that just don’t know about it.”

Currently, he said, companies are spending 90% of their time and money allocated for cybersecurity on defending against hackers, and 10% on responding to them. “We think that should be 60/40—or even more on the response,” Shofner said.

“There are very simple things that companies can do to keep people out,” he said. “Don’t allow workers to reuse passwords.” He noted that he had heard of a high-net-worth individual whose daughter played on a lacrosse team. A hacker found that out and used some of the wording from the team’s website to steal millions of dollars from that person’s accounts, he said. So, another good place to start is to warn people from using familiar places or things for their passwords, Shofner said.

He also said that in light of automatic enrollment, many participants check their accounts infrequently, if at all. Failing to do so on a periodic basis could leave them open to an attack, so it is a good practice for sponsors to remind their participants to check in on their plans.

Also, help participants set up their logins and require at least a two-factor authentication process, Shofner said. “To keep your data secure and your money safe, you do have to be somewhat engaged,” he said. “If you don’t log in all year or wait three years, your money might not even be there.”

Sponsors could ask their advisers to check to see if their participants are monitoring their accounts, Shofner suggested.

Finally, McDonough said it is critical for companies to train new employees on their cybersecurity policies as soon as they are hired, citing one case in which a hacker, using information from LinkedIn, posed as the chief executive officer to a new payroll coordinator hire at a Fortune 1000 company, asking her to send W-2s for all the employees. Companies also should restrict access to sensitive data to only a few people, McDonough said.

It is also important to have antivirus software, to do computer backups regularly, to update participants’ machines, to have cybersecurity insurance and to require those working from home during the coronavirus pandemic to have a virtual private network (VPN), McDonough said. “This

The bottom line, he concluded, is that cyberattacks are going to happen. “You have to know how to prevent them, what your response will be and where your liabilities are,” McDonough said. Using all these best practices and protocols, Shofner added, “screams that you are trying to protect your retirement plan and make a tremendous difference.”

Tags	401k, cybersecurity, Department of Labor, DOL
Reported by	Lee Barney
Reprints	Please contact the PLANSPONSOR Reprint Manager, Michelle Judkins.

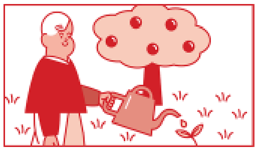
You Might Also Like:

COMPLIANCE | September 23rd, 2020

PSNC 2020: Preston Rutledge’s Inside View of the DOL

COMPLIANCE | September 23rd, 2020

PSNC 2020: Legislative and Regulatory Update Part II



INVESTING | September 22nd, 2020

PSNC 2020: Time to Get Serious About ESG?