Please note: This is an AI generated transcription - there may be slight grammatical errors, spelling errors and/or misinterpretation of words.

2026 Fiduciary Training Series, Part 1: Cybersecurity Risks in Retirement Plans Webinar

Lisa Caito: Good afternoon, and thank you for joining us today for the Cybersecurity Risk and Retirement Plans. Cybersecurity is one of the most significant and rapidly, rapidly evolving risk facing retirement plans with increasing regulatory scrutiny and real world incidents, underscoring the importance of strong fiduciary practices.

So today's session, we're gonna focus on the latest guidance for a qualified retirement plan. I'm Lisa Caito, the director of the Plan Consulting Team at CAPTRUST. Joining me today is Jenny Kiffmeyer, chief Operating Officer at the Retirement Learning Center. GI has been in the retirement services industry since 1993 and is a recognized leader in ERISA education, professional certification development, and award-winning industry content.

She's also the co-author and editor of the Retirement Resource Guide. Essential ERISA education and best practices for financial advisors and holds a JD from the TAF Law School. Before we begin today, let's quickly review a few housekeeping items so you know how to participate in today's event. This webinar is being offered for CE credit for both SH RM and CPE to be awarded full credit Hour.

You must be present for the entire session. Register for your attendance and departure in the webinar. In addition, you must answer three polling questions during the presentation. Failure to complete these three questions will result in no CE credit. You will be given 60 seconds to answer the questions and any questions you have related to the awarding of CE credits will be resolved after consultation with the retirement Learning Center's CE administrator.

And lastly, you are connected using your computer audio, and all attendees lines are muted in listen only mode. You may submit questions at any time by typing them in the Q and a box, but you can open or minimize using the icon at the

bottom of your screen. All questions will be collected and addressed after the event.

Today's webinar is being recorded and a follow up email with a link to the recording and a copy of the slides will be sent within a week. And with that, Ginny, I'm gonna turn it over to you.

Jennifer Kiffmeyer: All right. Thank you so much and thank you ha, for having me here today. And, and we would. We'll be talking about a very important topic of cybersecurity risks in retirement plans.

If we go onto the next slide we'll see that today we're going to, at the end of today's session, our goal is to be able to give you. An update on the latest guidance on cybersecurity protocol for retirement plans. Hopefully you'll go out, walk away with some tips for hiring plan service providers.

Also, what are some of the best practices for having a secure. Program in place for your retirement plan participants, and recognize how your plan advisor can really be helpful in meeting the cybersecurity goals for your plan. Next slide, please. I So retirement plans have become. Somewhat of an easy target, and it's, it makes sense because retirement plans today as of last count was at the, the balances were at.

$48 trillion. So this just brings to mind an old story about a 1930s bank robber by the name of Willie Sutton. And Willie became famous not just for robbing banks, which he did quite prolifically in the thirties. But when a newspaper reporter asked him, why do you rob banks Willie famously answered, because that's where the money is.

And cyber. Criminals have discovered that $48 trillion, that's a pretty good place to start looking for some assets. And because the retirement industry is supported with a lot of different providers, there's a lot of different touch points. If you think about it, there's the payroll, there's the, you know, the plan sponsor, there's the.

Participant portal. There's the record keeper, there's the trustee. The, so there's a lot of different areas where personal identifiable information of participants could be accessed by cyber criminals. So because we have all these different touch points that makes retirement plan assets somewhat of an easy target.

Next slide please. So let's talk about the guidance that we have available and if we move on to the next slide, we'll see that the Department of Labor does have

a regulation related to the electronic delivery of information and notices for plans that states that the plan sponsor must ensure the electronic system that it uses.

Keeps the personal information of participants safe and confidential. That's really all it says. It doesn't tell us how to do that. It doesn't say that it's necessarily a fiduciary responsibility, but it is something that the plan sponsor is tasked with. Now, you would think there would be some extensive guidance for us to turn to.

However, unfortunately, there isn't there is no regulation from federal agency governing cybersecurity for retirement plans. What we do have is some guidance. That was issued from the government Accountability office in 2021 suggesting that the Department of Labor should come out with some regulations related to this.

We do have state law that comes into play. I think there's about 47 states that have enacted cybersecurity laws. For business owners, not necessarily specifically for retirement plans, but in general. So we have some guidance there, but if we go on to the next slide we'll see that with respect to the Department of Labor, there really isn't any formal guidance.

What we have are some best practices and. I'll, I'll focus a bit on this case that kind of started the whole ball rolling, so to speak. With the focus on cybersecurity with retirement plans, this was a case Barnett v Abbott labs back in 2020. And what happened was a plan participant had her personal information stolen by er, cyber criminals.

And they were able to access her retirement plan account and go, you know, steal $245,000 from her account balance. What the criminals had done where they were able to get a security question from the planned record keeper and that they got the answer by. Logging into the participant's emails, got the answer to the security question, then logged in on the record keeping website, and was able to request a distribution.

Now in this case the plan participant was not able to get all the money back. She only was able to retrieve, I think, about $109,000 worth of it. The record keeper had given, given her a. You know you know, it came up with to her with a settlement proposal, but she refused it and was gonna hold out for the full amount, but they were o only able to recoup.

A bit of that. Now, most of the criminal cases that are happening today with retirement plans, the plan is we'll move to settlement. This plan didn't, this is one of the first, you know, cases, but cases since then, plans have been much more willing to settle and you know, provide you know, money back to participants if they've been hurt by the breach of information.

Next slide please.

As I mentioned, the Government Accountability Office issued that report. They were really, would like to see the Department of Labor state that it is a fiduciary responsibility to mitigate cybersecurity risks with retirement plans and also give some at, at minimum you know, a Safe Harbor guidelines for.

How plans should address cybersecurity. Next slide, please. Okay. What we got from the department. Labor of labor fell short of that. We have what we, you know, lovingly referred to as three points of light. There are best practices and there are three versions of these. Number one is tips for hiring a service provider.

Those are tips that plan sponsors can use when they are vetting. Plan providers and assessing their cybersecurity policies and protocol. So that's for the plan sponsor to use. There is a second best practice sheet and entitled cybersecurity program, best Practices that can be used by Plan, service provider.

So TPAs, record keepers you know, other payroll providers, et cetera, can follow those best practices and have some idea of what the Department of Labor is looking for as far as safety precautions. And then finally the third version is for participants, and it's called Online Security Tips. And it's really a list of dos and don'ts for plan participants.

For. Dealing with their own personal information and keeping that safe. Next slide, please. Ah, we're off to our first quiz. Now remember, if you are seeking a continuing education credit, you need to answer three questions. We have four throughout the presentation, so this is our first one. Next slide, please.

Our first question as it relates to cybersecurity, the Department of Labor's current policy is A, it has specific rules and regulations for plan sponsors to follow. B, it does not require plan sponsors to have a formal policy or procedures in place. C. It has guidelines for plan sponsors to follow it. Its best practices or D, both B and C.

And we'll give you a few moments to review the options and contemplate your selection for this first CE question.

So, as it relates to cybersecurity, the DO L'S current policy is.

And moving on to the next slide, we should see the answer is both B and C is correct, and the majority of you had this correct selection. Now I'll remind you that you don't have to get the questions correct, you just have to participate to get the credit. Next slide please. So let's move on to that first point of light from the Department of Labor, the best practices for plan sponsors in hiring a service provider.

Next slide please. So for this best practice checklist sponsors can use this to go through their vetting process with potential service providers for the plan. It's really going to help them fare it out, the important information, and it goes into six areas. If we move on to the next slide, we'll see that the six areas start with.

Asking about the service providers information security standards you'll want to just start questioning what are your standards? What are your policies and procedures? Can I get a copy of, of your policies and procedures? What about audits? Do you have a regular audit? If so, can I get a copy of that audit?

You'll see that at the top of each of those three boxes I have document, document, document. And that's not a mistake. That's really just repetition for a reason. It's to drill it in the idea that if. Documentation is so important because if, if it's not documented, it, it didn't happen in the eyes of the Department of Labor.

So that's why you know, for if, for asking on the service provider information, get copies of that information. The second one we ask have asked the service provider how they validate their practices. What do they do? Do they have a, a certain time schedule that they go through and run, you know, make practice runs on testing for security breaches or potential breaches.

On the next item, document the servers, providers track record. Have they had breaches in the past? Ask them about those breaches, and if they did, what were the remedies that they implemented? How long did it take them to? Fix those breaches. Next slide, please. This next one is kind of in, in tandem with tracking their former breaches is, you know, what kind of insurance do you have for cybersecurity breaches.

Now, you know, as you know, plans must have an ERISA bond. But those are that bond is to protect the plan assets. There's also, plans can buy fiduciary liability insurance. That is something that's o over and above the ERISA bond. And that fiduciary liability insurance protects the fiduciaries of the plan.

But often that policy does not cover cybersecurity per se. So there are. Specially designed cybersecurity insurance policies that can, the plan can purchase and it may be advantageous. Again, depending on the size of the plan, the risks that you assess might be there. It's not cheap, but it is something to contemplate given the risk factors that may be present for a plan.

Next we want to look at the idea of getting it all in writing. Again, ask for a copy of the insurance policy. Have them explain who's covered at what level and what kind of steps must be taken in order for the coverage to kick in. Get it all in writing. As I said, if, if it isn't at writing, it didn't happen in the eyes of the Department of Labor.

So we know that Department of Labor investigations have begun that include cybersecurity look looking into the cybersecurity practices of plans. What is the, the DOL is currently doing is if a plan is already under audit or investigation, in addition to the reason that they're looking at the plan to begin with, they will also.

Instigate some cybersecurity reviews as well, and there is a long list of documents that they are requesting. From sponsors that are in this particular situation. And it will oftentimes involve the plan sponsor needing to get documents from their service providers in o order to be able to answer the questions that the DOL is re questioning or the information, and answer the questions that the DOL has.

A very important note is if the plan sponsor cannot produce the requested documents or cannot answer the questions, they have to provide a specific reason as to why those documents aren't available and to as to why they cannot answer the questions. So again, the DOL is taking this very seriously. I know they have, the, the creation of re regulations on their docket on their agenda for the coming year. So we can anticipate more guidance, but if for the time being we know they are looking into cybersecurity practices, especially involving plan service providers and how the plan sponsor is prudently selecting those service providers as they relate to cybersecurity issues.

So next slide please. So some practical tactical actions for plan sponsors to take for protecting plans. You know, it's very important, again, you do have a

responsibility to protect employee and participant information. One of the key things that DOL looks at is payroll processing. They're very, very concerned about plans depositing.

Payroll on time and making sure it's going to the right accounts, et cetera. So get your payroll provider involved and making sure that the process is buttoned down and there's no room for error. One of the most common record keeping errors, believe it or not, is the actual you know, transmittal of.

Payroll to the wrong people. And so, you know, something like, you know, doing a check for that and making sure the payroll processor has protocols in place to prevent that. Also document the record keeping cybersecurity system and processes, procedures make sure that they've got you know, adequate.

Protocols in place to at least, you know, protect participant information. And moving on to the next slide you might wanna suggest too that they take a look at the Department of Labor's best practices that they have for service providers. And, alrighty, we're down to our next quiz. So this is question number two, and if we move to the next slide, our question is.

Plan, advise, excuse me. Plan sponsors should request documentation from the following service providers regarding their policies, procedures, and remediation practices for cybersecurity breaches. They should ask the payroll provider. B, they should ask for the record keepers documentation. C, their plan advisor's, documentation, or D, all of the above.

And here again, we'll pause to give you time to reflect on the question and consider your selection A, B, C, or D. And a reminder that you don't have to get it correct, you just have to participate. And that shows the CE board that you are actively participating in this event today. So we have just a couple of seconds left.

If we move on to the next slide, we'll see that the correct answer is DA D. 98% of you got it. Correct. Good job. Next slide please. I so let's look now at that best practices piece from the Department of Labor. For plan service providers, this one's a little more in depth as you might imagine, because plan service providers are the ones that are actually managing and controlling a lot of the participant information.

Next slide, please. So this is again, again, a best practices checklist for providers they can go through and make sure that they're at least meeting this minimal or

these minimal suggestions on their best practices. Next slide. There are about a dozen suggestions here. So first off, it's number one.

Have a formal, well-documented se cyber security program in place because you know, you're sponsors are going to be asking for that information, so you might have, might as well have it. Documented and available for distribution. You should co conduct prudent annual risk assessments. Oftentimes that means you should do this on a, on a, and have it scheduled on an annual basis.

Sometimes these tests are conducted quarterly. So at least an annual risk assessment, but more often if the provider feels it's necessary. Number three, have a lot of reliable third party audit. Of security controls. That's almost you know, a mandatory provision. You might have heard the terms, the SOC one, SOC two, SOC three reports.

Those are going to come from a third party that looks at the providers cybersecurity practices and procedures and make sure that they meet. The industry standards. So from a plan sponsor's perspective, asking for the providers, SOC one and SOC two reports is very important. SOC one is gonna be the most important to get because that's going to give.

The auditors report on the security protocols in place and whether they meet specified standards. Number four clearly define and assign information security roles and responsibilities that's necessary so we know who's responsible for what and who should be contacted. Who should the plan sponsor be contacting if they notice there's benefit.

Security breach related to the plan. Next slide, please. Number five have strong access control procedures. This is where oftentimes there's going to be at least dual authentication, if not more. I know that some companies only will have you know, one level of office education. Some companies now require two.

So the more levels of security. The better. Even though I get frustrated myself when I, you know, have to go through a certain number of levels of authentication I try to remind myself how very important it is because a lot of dollars are at stake, and so it's important to have these dual and triple, et cetera authentication processes in place.

Number six. Ensure that any assets are data stored in the cloud or managed by third parties are, are appropriately secured. And we have an independent security assessment of the storage facilities as well. Whether you have your own

server internally or if you're using the cloud to store data, very important that that is also secure.

Conduct. Periodic cybersecurity awareness trainings among the service provider personnel so that everybody's on the same board and on board singing from the same hymnal, knowing what's the newest steps and procedures that they have to follow. Number eight is to implement and manage a security system, development lifecycle or an SDLC program now.

You don't necessarily need to know that as a plan sponsor, but the question, do you have an SDLC program in place is an important question for vetting the the plan service provider. Next slide, please. So number nine have an effective business resiliency program in place. And this is for should god forbid, a security breach happen.

How is it handled? Who gets notified? How is it shut down? How do, how are info plan sponsors and participants informed all of that. Should be outlined in a resiliency program and documented. And again, that would be something that a plan sponsor could request. 10 make sure all the information is encrypted.

That is something that I know my, my company personally, we just met, made sure in the last two years that every access you know available access where data comes in, comes in in an encrypted format. Number 11 implement strong technical controls. So that again, that you, you know, are checking the security of the practices that you have in place and making sure that they are indeed doing what they're supposed to be doing.

And number 12, of course, appropriately respond to past cybersecurity incidents. And part of that response is really how you deal with how the plan service provider deals with its clients, the plan sponsor. We had a, a, a cybersecurity breach several years ago where the provider did not, would not give us information.

They kept us in the dark for a long time, and that just. Made for growing suspicion and lack of trust. So important that your service provider address the need to inform constituents on a, a, you know, very active and you know, frequent basis. Next slide, please. Oh, we're onto our third quiz. All right, moving on to the next slide.

Our question is true or false plan. Sponsors should write, require written policies, and all insurance contracts should be obtained from their service providers regarding cybersecurity. Is that true or false? As a best practice, what

do you think? Should you get? Written policies and copies of the insurance Pro care contracts from your service providers.

And again, just a few moments to give you ample time to respond. Sometimes our computers are a little slow and we click on things, or a glitch happens, so we wanna make sure everyone has time to answer these questions.

And we're getting down to the last few seconds, so record your response and we'll move on to the next slide to reveal the correct answer is.

Absolutely. It's important to have that for your file and that again provides defense that you indeed went through a very thorough process to prudently select the service provider. Next slide, please. So, here we go. Online security tips. For plan participants. This is the third and final best practice that the Department of Labor provided for our use in protecting plan participant information.

And it's interesting because the, there's a number of studies that have identified the individual participant as the weakest link. In these cybersecurity breaches. And the reason for that is, you know, it all kind of starts with us as, as individuals, you know, being on on the web and taking care of our own personally Identifi information or PPI.

Next slide please. So here what we learned from the Department of Labor is that important for participants to be aware that they can, you know, be very active in protecting their own information. So if we go on to the next slide, we'll see that the first step that can happen is, registering and setting up your online account with your retirement plan provider. So this is the benefits website where you go in and sign up and make sure all the information on the account is up to date, you know, remind participants to do that. I'm, I'm very surprised at the number of participants, you know, new participants coming in.

Who failed to set up their accounts, and that just is a, you know, a, a problem waiting to happen. 'cause should. A cyber criminal, be able to access an email that happens to have the, Hey, welcome and join the, or the online community for the benefits and enter in information and they're off to your, the participants benefits. So again, encourage participants to make sure that they update. You have, number one, register online for their account. And number two, keep that information up to date. As part of that registration process, use strong and unique. Passwords. You know, the password thing is probably the, the area of where most errors are seen.

Make sure that you know, you are using a long you know, password. Don't repeat passwords. Don't use the same password over and over, across different, you know, venues make sure that it's unique. Don't write them down. It's better to use you know, the, the live, the booklet, online booklet to keep them your, your passwords safe.

Rather than writing 'em on a sticky note and sticky 'em to your screen, or having a written diary somewhere available that has all your passwords that just is, is too easy. To take advantage of use multi-factor authentication. I've seen that more frequently now, where you're given the option when you're signing up for a, an account, not just your, your plan account, but maybe you know, some other kind of account or app, app on your phone where they give you the option to use multifactor authentication.

And I know it can be frustrating, but it is a level of security that could be very much appreciated down the road. Next slide please. We also encourage info or participants to keep their personal contact information current. So that means going through and updating on the account, you know, your phone number.

I just had to do that today. I had an old phone number on my, one of my accounts. And should there have, you know, might there have been a breach of information, the call would've gone to my old phone number, so. A key point updates your information so that the plan, sponsor and record keeper, et cetera, can get a hold of you as a plan participant or beneficiary.

Here's one that I often don't think about is close or delete unused accounts. You know, you may have thought, oh, this looks like a good account to set up, and then later on it's like, no, I'm never going to use that. But then you've got this old account setting out there best to delete it. Because someone might stumble upon it, be able to crack into it.

And through that information, that login information might be similar to log information that you've used in other accounts. And that could lead to a you know, domino effect of c. You know, being able to enter into other accounts that the participant may have. Next up be wary of free wifi. Now I know our own company computers that we use, we cannot use free wifi to access and do any work, access any accounts via free wifi.

That's just a security. Protocol that they have put in place, but not all companies are like that. Or if you're using your personal computer to access accounts you know, as a, as a plan sponsor or as a participant, be wary of that free wifi

because it's very easy for information to leak out and others to crack into your information and your data.

Next slide, please. Be aware of phishing attacks, and these are getting to be so sophisticated these days. You know, phishing is usually, you'll see, you'll get an email. You'll, you'll think, oh, it's from somebody I know, or it's from a business I know. Or it says urgent IRS, you know, seeking your, you know, U four a refund, s something that's going to catch your attention.

Make you lower your guard and make you click on that email and, and or link. And once you do that, you're opening yourself up to a cyber criminal, being able to access your data. It used to be, you know, easier to spot them because you'd see oh, it's, it's, it's the IRS, but it's got a weird email address or a return address or some misspellings are in the, the title or the email.

I got one from good friend of mine. That, you know, I wouldn't have thought twice of except he, the email was signed. Talk to you soon, Andy. And it's like. Andy has never signed an email like that, so I knew something was up. Anyway, just be on your guard for these phishing attacks. It's an easy way for cyber, cyber criminals to, to get access.

Next up antivirus software. Keep those up to date on your your computers, your desktop, your laptops your tablets, all of that. Keep that antivirus up to date. And then know how to report. Any incidents of cyber theft, whether it's your ident identity or you've noticed something strange, some strange accesses to your account?

It's nice nowadays. You know, oftentimes for certain services you'll get notifications via email or text that says, Hey, did you just access so and so account? If not, if so, disregard. But if not. Please contact us because someone has been trying to access your account. So make sure you know how to report the theft.

And that's going to depend. Two on, you know, if you are a participant in a plan, you're going to go to the HR department, probably first. Also the record keeper. Next, report it to the plan sponsor. So the plan sponsor then can escalate it to the next level, you know, plan, sponsor. But probably if it's a large enough or, or concerning enough.

Breach or something that that hasn't already been handled. Some it may be necessary for the plan sponsor to escalate it to the Department of Labor and potentially to the FBI. So know who to report any kind of incident to Next slide.

The role of the financial advisor in cybersecurity. I always joke around with the attendees on, on webinars that I could barely spell it.

So if I were on a plan committee or if I were a plan sponsor and had to make decisions on cybersecurity information. I'd be dead in the water. Deer in the headlights. So here's where I suggest that on the plan committee, if you are lucky enough to have a plan committee or if it, if it's just the sponsor and maybe HR professionals involved with the plan is to enlist the services of your financial advisor who could help to point you to a cybersecurity.

Expert. Maybe you've got someone in-house that could serve on the committee for the plan or at least be enlisted to help interpret the cyber information that you, or security information that you'll get from the plan providers. Next slide, please. So other ways that the advisor. Can help support plan sponsors is to you know, just get a governance policy in place and make cybersecurity one of the items that is regularly reviewed as part of an overall governance.

Process. The advisor can also be very helpful in gathering the written documentation from the service providers that you have from the plan. You know, here again, go down that list that's on the best practices checklist to get the policies. Procedures, best practices, et cetera, from the service providers.

You know, ask again those key questions, the advisor can help you ask those key questions about, you know, do you, does the provider have a dedicated cybersecurity resources in place? And how much have they invested in cybersecurity? This, the advisor can help ask those difficult questions.

Next slide, please. Further advisors can really play an important role in educating plan participants. And remember I mentioned that participants are often the weakest wink link weakest. Link in the process. So education is so very important both for participants and, you know, for the plan, sponsor and committee.

So as far as education for participants, have the advisor schedule and education session where they introduce the DOLs best practices for participants so you can go through those. Tips to keep information safe. Help the participants understand how to protect themselves and how to report any incidents that they come up a across.

Don't forget to document. The educational efforts that you take, that's very important. Again the Department of Labor, if you were to come under audit, may ask for information that you have both been educating your participants on

cybersecurity and that you've been keeping the plan committee members up to date on plan cybersecurity protocols, and also all that documentation you've re requested from your plan services.

Providers make sure that you're, you know. Talking about this on a regular basis with planned participants, or even, you know, my company is, is famous for sending out sample or yeah, sample phishing emails to see if anyone bites. They're doing it in, in, you know, with the hope that no one gets caught.

But if they do, it really helps them. Number one, draw attention to, you know, for the participants to. Really beyond their, our, their best guard. And then also to make sure the protocols that they're following in house are working. They can judge. Okay are, you know, we've been giving training. How is it working?

If our, a lot of our individuals are failing, then we've got to do some changes in our training process. Next slide, please.

I think here is another area where advisors can be very helpful and it is interpreting or demystifying the service contracts from providers. Get it, you know, in writing and then review it. Have your advisor walk through the different service agreements. And policies and procedures insurance contracts, so that you all have an understanding or a better understanding of what the service provider has is providing what they, you know, what coverage they will provide, who's covered.

And so it's again, you know, very helpful to have that advisor helping you decipher all this information. Next slide, please.

Now I mentioned cybersecurity insurance and recall, we've got our everesa bond for the plan. That's mandatory, but that is something that doesn't necessarily address cybersecurity breaches. Separately, we have what's called fiduciary liability insurance. Something additionally that a plan could purchase to cover the fiduciaries of the plan so that in the case where there has been a breach, the fiduciaries would be covered for personal you know, the personal liability under the plan.

Very often those fiduciary liability insurance policies do not address. A, a cybersecurity breach. And so it's very important to make sure that you either get an additional rider for that insurance policy or you go to the third level of protection and buy a cyber security insurance policy specifically for the plan and plan assets and plan fiduciaries.

That, that third bullet consider the need for first party coverage. So you'll see that with that cybersecurity insurance, there's third party coverage, so that's going to, you know, cover the service provider in the breach. But the first party coverage is going to cover the plan sponsor and committee members involved with the plan.

So now with that said, it's not cheap, and I think I mentioned earlier that you know, you'll have to weigh the, the, the pros and cons of, of needing or wanting this insurance with, you know, the cost of, of getting it. And if you. Look through the cybersecurity procedures of your plan service providers, and you feel that it's very tight and meets those best practices suggested by the Department of Labor.

The need for additional service probably goes down. It all depends on your level of you know, risk tolerance. Next slide, please. Ah, we have our last question opportunity here again for CE purposes asking you to answer at least three. So this is our fourth option for a question. Which of the following is a cybersecurity best practice?

Is it a have a formal, well-documented cyber program in security program in place? B, conduct prudent annual risk assessments. C, have a reliable annual third party audit of security controls, or D, is it all of the above? And again, we'll pause for a few moments here, let you think about the options, and then select your answer for which of the following is a cybersecurity best practice.

And we're counting down to the reveal of the correct answer. So register your answers quickly here and we'll move on to the next slide to C, that the correct answer is D, all of the above. That is absolutely correct. Next slide please. So in closing for today we have a few key takeaways. Just to remind you that right now there are no formal Department of Labor guidelines for plan sponsors to follow when it comes to cybersecurity and the practices and procedures that need to be in place.

There are some regulations that are being prepared right now. They have not been released. We don't know what they say. They're in the work. So we may see something later on this year, but right now there is nothing at the federal level. We do have some guidelines from the department of Labor.

We also have some guidelines at, at the state law level that sponsors can take a look at to try to implement some cybersecurity procedures for their plans. But right now at the DOL level, we have those three best practices, worksheets, or

checklists. One for plan sponsors, one for service providers, and then one for plan participants.

Make sure to have access to an IT professional whether it's someone in-house. Or someone you bring in, maybe your advisor to the plan can recommend someone. But a lot of times the information that on cybersecurity and IT security protocol. Is very difficult to understand. A lot of acronyms, a lot of strange words that I don't understand and many folks don't.

So don't be shy. Get someone who can understand and help you interpret those that information. So we can avoid any breaches and make sure that you know, your plan, number one doesn't come under. Con, you know, under audit from the Department of Labor or you lose assets and be, you know, have face a lawsuit.

One thing we have noticed you know, I mentioned the Abbott case and that case was in 2020. There have been a number of other plan. Lawsuits involving security breaches. As I mentioned, most of those lawsuits have been settled by the plan sponsor rather than going through the entire, court process they've been able to the plaintiff has been able to bring a case show that there is valid cause, and rather than go through the, the cost of discovery and the cost of a full trial they, the, the, sponsors and record keepers and other service providers in these cases have chosen to settle.

Some of these settlements have been in the tens of millions of dollars. And the other thing just to mention, just to, to drive home how very important this information is, is the number of data breaches that have occurred, let's see, I think in last year there was around 3,100. So 3,100 cyber data breaches that occurred now that doesn't maybe seem a lot, and we had this a, a similar number this year, but the number of victims has dramatically increased.

Last year it was around 419 million. Individuals. Now, this is not just retirement planned breaches, but these are breaches overall. So maybe some of the, you've heard of the larger healthcare providers having breaches. I just, yesterday I heard the IRS had a breach of taxpayer ID information. So these, these breaches are becoming more frequent and the number of people who are being impacted.

Are growing from 419 million last year to 1.3 billion individuals being affected. And the, the, the key thing is just some very basic steps starting with your, you know. Safeguarding your own personal information can go a long way to preventing this. So with that said I'll, I encourage you if you have any questions,

to put those in the chat or submit them afterwards, and we can address those questions after the the session today.

You will be getting a copy of the deck and the recording as well. And so in order to get a copy of those three pieces from the Department of Labor you can request those through CAPTRUST RLC. My company makes those available. They are also available, or a version of them are also available online at the Department of Labor, so you can download them there as well.

And with that, I will turn it back over to Lisa, I believe to close out our session.

Lisa Caito: Jenny, thank you so much. This was such, such a valuable information. As we all know, the bad guys are out there and clarifying the guidance. Best practices is an important role for all of us to protect our retirement plan data and assets.

So thank you. Again, just some, a little bit more housekeeping as a reminder to receive CE credit. Please be sure you completed all your polling questions. You answer the survey, and you've remained logged in for the full session. The webinar recording will be available via email next week. Along, along with all the related materials.

And on behalf of CAPTRUST in the Retirement Learning Center, thank you again today for attending today for your time and your engagement. We appreciate it. Have a great day.