CPA
Practice Advisor

Clients – Apr. 2024

Hosts Randy Johnston and Brian Tankersley, CPA, discuss cybersecurity issues and strategies for managing high net worth clients.

Brian Tankersley • **Randy Johnston** • Apr. 11, 2024

Hosts Randy Johnston and Brian Tankersley, CPA, discuss cybersecurity issues and strategies for managing high net worth clients. Use the video player below to watch, or the podcast player below to listen to the podcast.

0:00

Or use this podcast player to listen:

0:00 / 24:00

Transcript (Note: There may be typos due to automated transcription errors.)

Brian F. Tankersley, CPA.CITP, CGMA 00:00

Welcome to the accounting Technology Lab sponsored by CPA practice advisor with your hosts, Randy Johnston, and Brian Tankersley.

Randy Johnston 00:10

Welcome to the accounting Technology Lab. I'm your host Randy Johnson along with co host, Brian Tankersley. Today we're pleased to have a special guest with us Rahul Mata, who's a Partner at isern advisory group. And he's going to talk to us about the five cybersecurity risks for high net wealth individuals. So, Rahul, would you like to introduce yourself please? Thank

00:33

you very much, Randy. It's a pleasure to be here with you. By way of background and introduction, my name is Rohit mana, and I'm the managing partner of iser, Amber's outsourced it practice. Our mandate is to protect our clients by using best practices of what we're seeing out there today. What's happening in the industry, what's happening with governance and compliance and putting a solution together to robustly protect the clients in all aspects.

Randy Johnston 00:59

So as you as you as our regular listeners know, our sessions on security are basically

some of these ideas, and topics are coming from what we're seeing within the firm and within our client base. And so with that, one of the overall things that we are seeing is, a lot of our high net worth individuals have multiple bank accounts doesn't sound unusual to have a few. But even in my personal life, when I talked to my family, about two years ago, we found 15 bank accounts that were scattered around. And so that does create a hardship for the financial advisor, whoever that might be. But it also creates a hardship to protect all of those assets. So one thing that we are trying to increase awareness around is if you have multiple bank accounts, if you're advising folks that have multiple bank accounts, it's really hard to centralize the security of those or to feel good that you have something simple such as multifactor authentication in some manner that you're accessing those bank accounts, you can set those procedures up for one or two. But if you expand out to 15, obviously, your beta increases your risk profile increases. So taking a look at where all your assets are and trying to consolidate them a little bit to create a heightened cyber awareness. Thought Process is one of the topics we're looking at right now. And

Randy Johnston 02:59

makes sense. Now Brian and I have talked multifactor for a long time, is there a particular platform that you're recommending to the clients?

03:08

Well, here's what we're seeing, we're seeing clients are deliberating between using the multifactor platforms that they get for free and some that they pay for, we typically don't provide guidance on which is the right platform, we just like to make sure that they're using a platform that is enforced and supported by usually the financial institution that they're dealing with more than anything. That's where you really need to start with the security of the multifactor. And then of course, having a strong password after you MFA is really the next barrier to have.

Randy Johnston 03:46

things in your world.

04:12

Wonderful. We have found a lot of individuals try to get involved with currency in whatever cryptocurrency as you mentioned, they might be involved in I think the the challenge over the last few years is how do you get involved and so some of the advanced I would say clients of ours went directly and created wallets on their own. And then probably a couple of years ago, coin base became popular to have a more of a public and easier wallet to use and, and so there became challenges with that. And so I think that overall, people have different approaches. I think the third evolution now is you can actually go and buy an ETF which just started in the last few months to make it even easier now. The first few iterations to answer your question, the challenge we came on how Been a secure way to keep your wallet in place. And so was it a USB stick where you'd put your code on and keep that USB stick? Well, we found some of our early clients, those USB sticks were getting lost, they forgot them or somehow gets stolen. And they're those x 1000s or millions of dollars. The second way was using a platform such as Coinbase, which is still very popular. And, again, you have your password challenges. And so you know, an advancements there we've seen is trying to suggest using a third party tool like a YubiKey. And UB keys, I think, are really a much stronger way to do it at a very low cost point. You can buy that key off Amazon these days for $50 or less. And I like that a lot. If you're going in. I see you have one right in front of you. So we're talking the same thing.

Randy Johnston 05:51

Yeah, in fact, we both known Steena ever insurance, she created those products. And we did cover those in our CES presentation a little earlier. Prior podcast, so so it makes perfect sense to use these hardware keys to us as well.

06:09

Yeah. So I think now with the ETFs I think that makes a obviates a lot of the security

06:42

With, if I can, I'll take a step back and put some context around it. So taking an elder generation, like you mentioned, your mother in my elders as well. They started off probably around 2000. And they that's back in the days where you used to get those CDs coming to your home, and you know, those lovely, those sounds that came from your US robotics modem, and you would dial in and you'd get your AOL email. And that's where many many folks started getting their email accounts. And now fast forward, it's the year 2024. So you got 24 years, AOL kind of became, you know, your, your habit. And so many of that generation used AOL, for example, is just focus there. And so they have 24 years of pictures of chats of email history. And so they're very attached to using that archaic technology. The reason I called archaic is AOL has been bought and sold multiple times over that 25 years. And so the effort to increase the cybersecurity platform and hygiene around that platform is not as much there and then focus anymore. And so we just had a recent case where a clinic came to us where they had, they were a victim of some identity theft. And really the issue was, they had been corresponding with their CPA for 24 years on AOL, they had 24 years of tax returns in their AOL account, 24 years of PII information of them in their family. And so that data all became compromised. And truly, because, you know, nobody really is focusing on AOL, and heightened security and new, you know, ransomware techniques. And so, you know, it becomes a problem. And I understand the shifting, emotional cost is high for that individual, because they don't want to lose 24 years. But the risk return is incredibly unbalanced right now, using those technologies.

Brian F. Tankersley, CPA.CITP, CGMA 08:45

You know, I completely agree with you. And, you know, I've talked to a number of practitioners, and I've, I've said, I've told them, and I've told anybody I talked to you that nothing says I'm not serious about cybersecurity, and your privacy, like a CPA

But just a reminder that the dot CPA domain may be a way for you to increase your security if you're a public practice firm. So we have talked about that in prior sessions as well. It's

09:52

well said I completely agree with that, that comment and for those that want to buy Your domain or get secure email, you can go to microsoft.com. And it's $5. And so that investment, I think, just, you know, is well worth it. Yeah, I

Brian F. Tankersley, CPA.CITP, CGMA 10:11

mean, it's not like we're talking about a big spender thing here. You know, it's just, it's, it is painful to make that switch. But there are tools that, that consultants and managed service providers like Eisner can help you make that switch and pull in all that content and everything else. So talk to us about family members, you know, it's family is just seems to be the gift that keeps on giving, especially when we get money involved in it. Talk to us about that.

10:39

I love the way you say that the gift that keeps on giving. There's so many wonderful things about having your family and being involved with your family. I was part of a family business for 20 some odd years before joining Eisner. And I think it's wonderful that the downside that we see from a cybersecurity perspective is not all family members have the same heightened security awareness that other family members do. And the balance becomes how do you how do you handle those family members. And so some examples of that risk that we continually see from our financial advisors and our accounting team members trying to handle these situations are starting off with just password management and understanding the risk of having really weak passwords and allowing weak passwords to exist in a family office, for example, and how you do that. The second aspect that we see is just

where you thought a photo is safer. Many people have historically thought a photo is safe, it's really not anymore. You

Brian F. Tankersley, CPA.CITP, CGMA 12:31

know, I completely agree with you on that. And one other caution, I would just mention that I'll just throw in since you mentioned iPhone, by default to your iPhone and your your Android phone both do something called geo tagging on photos. And so what happens is it puts your latitude longitude on there for photos. And so when you post things on social media, like you go to your grandkids house, your grandkids home to see them. Guess what, somebody that's a cyber criminal now can go in and look at those photos on social media that are shared publicly, they can right click and look at properties. And there's the lat long of where that kid is. And so they may inadvertently be making those children effectively a target for some kind of crime to get at get a ransom or other things like that.

Randy Johnston 13:18

And your point about the quality of the AI in the iPhone image scan is pretty stunning. You know, Apple, of course, has purchased over 30 AI companies. And in my experimentation with it, I've actually searched on something obscure like dinosaur, and a small toy dinosaur in the corner of the image is recognized. So you can absolutely guarantee that the image recognition across the Microsoft Windows platform, the Google platform, or the Apple platform, actually, I think increases the risk, as it turns out. And when you know, you consider the data exposure, Brian, which you and I have talked about so many times with the MailChimp exposure instead from Intuit. And now with Google potentially buying HubSpot. You know, both of those transactions are, you know, data mining as far as I'm concerned. So as practitioners, we have to worry about protecting our data. Just like Rahul, you're talking about it in terms of high net wealth individuals here. We have kind of a loosey goosey approach to protecting data here in the United States. So that'll change

a little bit more heightened awareness from, I would say, financial professionals or clients themselves. And I would say C suite. And so with that, I think there's been some cases in the last year where the C suite was held liable on a personal basis for having poor information security policies, and I would say, acting in a general duty of care to those stakeholders and shareholders that they're involved with. And I think that's a that's a real turning point in my mind over what's happened in the last year. drizzly was one case where the CEO was was found liable. I'm not sure if you know about that case or not, we can talk about that. I think the the, the Uber CTO a couple of years ago, having some personal liability attached to their lack of care, I think is another aspect. And I liked the new provisions about if there is a breach of much more heightened awareness to to disclose that breach, otherwise, you can be found, you know, not acting in the right care as well. So I'll just take a pause there. And I know I went a little off topic, but it's definitely something we're seeing a lot more this year.

Randy Johnston 16:26

Yeah. And as you were talking about that rule, I was considering, you know, Brian has written a session for our K to business called AI confidential on privacy and artificial intelligence. And many of the regulations around that, again, probably a little off the topic for today, but it was stunning. What was inside some of the license agreements, the ethics statements, and so forth, them a variety of it.

Brian F. Tankersley, CPA.CITP, CGMA 16:56

And when you read, the other thing that folks need to know is that when you start reading the pronouncements like the executive order that President Biden came out with last November on on AI and privacy, and you listen to some of the comments that have been made by the the commissioners of the FTC and other organizations like that, it's very clear that that privacy regulation is coming to town, whether or not it can get through Congress one way or another. Yeah. So it's a it's I think that's

standards, from this year, you know, the NIST framework getting updated to two Oh, finally, those those are some pretty radical shifts. While we're, you know, in terms of just thinking things through, are there any key recommendations that you'd make? I guess what I'm looking for is just, if you could only do one or two things, what might those be in

18:20

relation to an individual a financial? Like? Who would who would I be giving that advice to?

Randy Johnston 18:27

Yeah, let's keep it over on the individual frame for just a minute. And then we might turn it to business. Yeah,

18:33

yeah. So on the individual side, I would probably have more than one or two, but I would say, just be a little more thoughtful about where you are. So on the individual side, I would say our perspective used to be protect the castle. So individual went to an office or a place of work that was secure. It's important for the individual to realize they've left the castle, they've left the means and bounds of security that were around them, the moats that were protecting them, and now they're on their own, really. And so our framework has been to protect the individual now and how do we think about that and so when an individual travels, you know, often all of us go to airports or train stations, you see people working, because all we do is work the now in this country all the time. And so connecting to a Wi Fi, just because it says free Wi Fi, you don't know who is promoting or sponsoring that Wi Fi, it could be a hacker sitting right next to you with a free Wi Fi spot Wi Fi calling it free Amtrak. And so I think just recognizing, you shouldn't just use anything that's free, whether that's a

Wi Fi, whether that's a charging station, I often see these devices blokes that have all

you are using your password structure. So that's a long story, perhaps not one or two, but just in general, a heightened awareness of who you are, where you are, what you're doing is the most important thing. No,

Randy Johnston 20:47

I appreciate that. And if you were to likewise give just one or two ideas about primary business protection, what might you give there?

20:58

On the business side, again, I think it's back to not protecting in the castle, but protecting you know, where individuals are. And so with that, I think the compliance landscape is entirely changed. Both of you said it far more articulate than I did, and you know the exact role in numbers that they are. I just know in general, from our perspective, at iser, from our professionals, we are all much much more concerned about compliance regulation and governance in general, performing risk assessments is something that we start our conversations always with, I always say it's measure, manage and monitor. And so the first step is, in our engagements and talking to whomever we do is how do you measure your risk? Whether you're trying to measure your, you know, risk to meet an SEC standard? Are you measuring a risk to meet your cyber insurance, which is some just basic things, you have to really measure where you are, as Brian said, a third party I think is much better than just asking your IT department to go check a list or your current MSP get a third party to check off where you are in terms of your compliance or internal your cybersecurity, and just some of the basic things I can't tell you how many people still, our companies are not educating their own employees. So doing cybersecurity training, we did a recent survey, I think almost 40%, roughly, of our companies aren't even doing it annually. And so in that survey, it's mind blowing to me, how people are not just educating their their general shareholders, stakeholders that are involved in that

No more than anything, I appreciate you being here, Rahul. It's nice to have someone of your stature and of your firm's. You know, one of your firm's leaders join us here on the podcast. If folks want to have a further conversation with you, how can they get a hold of you?

23:09

Very simply, if you go to our website, iser ampere.com that you can go to to outsource day T, you'll see a lovely big picture of me. And it's pretty easy to get a hold of me if you put my name in to Google. It's right there. I think also in this podcast, we'll have some information that's available and as a free resource. We just released a cybersecurity ebook that can help individuals I know it's listed on your website in the download section. And so that's another great asset and tool and from there, you know, our team can be reached as well.

Randy Johnston 23:40

Well, that's super well. We appreciate all of you listening in today and we look forward to having you in a future accounting Technology Lab. Good day.

Brian F. Tankersley, CPA.CITP, CGMA 23:51

Thank you for sharing your time with us. We'll be back next Saturday with a new episode of the technology lab, from CPA practice advisor. Have a great week.

= END =

Security • Technology