ACCOUNTING

The Technology Lab Podcast – Safeguarding Client Data: Update on IRS Pub 4557 – August 2023

Technologists Randy Johnston and Brian Tankersley, CPA, discuss client data security and the new FTC Safeguards Rule: IRS Pub 4557.

Brian Tankersley • **Randy Johnston** • Aug. 16, 2023

Technologists Randy Johnston and Brian Tankersley, CPA, discuss client data security and the new FTC Safeguards Rule: IRS Pub 4557.

Use the podcast player below to listen.

0:00 / 23:07

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

SPEAKERS

Randy Johnston, Brian F. Tankersley, CPA.CITP, CGMA

Randy Johnston 00:03

Good day. Welcome to the Technology Lab. I'm Randy Johnson with my co host, Brian Tankersley. And we're going to talk about a compliance issue that we have discovered that many firms have not met. And that is the FTC safeguards rule, which went into effect July 9 of 2023. And the supporting document of IRS Pub 4557. Now, as it turns out, we're going to use a lot of code numbers here with you, but most of you who have done tax are used to hearing it that way. And for me, I've traditionally started with pub 5293. Now the reason I like fit 293 is it's a beautifully written document. It's relatively short, only about four pages long. And it refers to 4557. And it refers to the National Institute of Standards and Technology, the NIST document on security. So Brian, and I realized that we thought most everybody would have had the compliance work done on this by the December 31, of 2022 deadline, but there was some misinformation that small firms didn't need to comply. And the rule of thumb is if you have a P 10 number, you need to comply with 5447. So, you know, Brian, I know that you've got some background in this as well. Obviously, we've written coursework for our K two businesses historically on this, and we've discovered some other courses that are good. So what do you think our tax preparer friends need to know?

Brian F. Tankersley, CPA.CITP, CGMA 01:39

I think they need to, you know, I think they need to understand this is a serious set of regulations with serious teeth. And you can get in trouble not only if you have some kind of data breach, you can get in trouble even if you don't have. Okay, so what I'm going to suggest to you here is that this requires a disproportionate number of things. And I'm going to quote from a god article from from February 1 of this year by Karen Nakamura, the, the bitly link for that is bit.li/day away FTC at bit.li/j away FTC. And so this kind of gives you some information in here. You know, gramm leach Bliley has affected accounting firms for a while, but the Federal Trade Commission now has decided that they are going to be the nation's privacy's are, much like the European

Union, Canada have these privacy commissioners or privacy ministers in many of those countries. As we look at this, though, it requires you to designate a qualified individual to implement and supervise the, again, in the Information Security Plan, you have to conduct a risk assessment, you have to design and implement safeguards to help control risks, implement access controls, you also have to conduct a data inventory to identify where were what is accessing customer information, and how it's stored, have to encrypt customer information in transit and when stored on the system, which is a new requirement. And we've been recommending for years that you encrypt your local hard drives, for sure, and your in your server hard drives in most cases. But you know, this is a new thing here. That to be required to do. So. Assess internally developed, and third party apps use to access information and that by the way, that includes cloud applications. And that means that you're going to have to dig in and read that privacy policy and the and the terms of service for your cloud applications. And in particular, I'm going to tell you that the one for QuickBooks Online, the combined there's about 48,000 words, okay? So you need to understand those things and kind of understand what the what the rules are there. multi factor authentication securely to secure disposition of customer information, change management, protocols, log user activity, test, the safeguards are monitor the safeguards during personnel. And, again, keep this keep this current. So this is a pretty healthy set of rules to get to well beyond the basic plans that many of you set out a couple of years ago, when this topics first came out from from some IRS publications.

Randy Johnston 04:37

Yeah, so Brian, you know, the the point here is that all firms should have had a written information security plan sometimes just called the wisp and many plans have been created, but there are requirements now specifically around the plans. Now again, Brian and I are going to provide you many Bit ly links and resource versus to solve this particular issue quickly. But the reason we thought it was time to put it again in a podcast was so many firms had not completed the work, which was stunning. Now, let's, let's frame it up for you. Because we want you to start with 5293, which gets you to 4557. Now, 5293 is a very simple read, it's only about four pages long. 4557 isn't much worse, you know, that particular publication is only 22 pages long. So you know, the two are written very, very well. But then it calls out the tasks that you need to do. Now, a couple of pieces of guidance. First, there is a pub 5708, that was put out in August of 2020 2022, I'll get it out. That really describes how to write the plans. And it's a gorgeous example. And there's just lots of things about 5708. I like, but I was asked earlier this year to help create a 4557 course, which is

posted at the Grove, and Brian and I also have the bitly link for you on that as well. But the grove course is about well, it's covers every topic that you need to really worry about. And it's at BIT dot L y slash 4557 corpse. Now, again, there's lots of people that are trying to sell plans that are canned, and they're charging, you know, a few $100 to $1,500. And I've actually looked at a number of these plans that were three and five and $700 in concluded most of them actually won't get the compliance done for you. So you need to go through the steps that are associated with this. But the last piece of teeth was the July 9 implementation of the fines. And the July 9 safeguard fines come out to be the class of $100,000 per firm per incident, and $10,000 per partner. So even if you're a relatively small firm, if you have a violation that's assessed a penalty, a sole practitioner here could be in the $110,000. class. So, you know, my take when I look at those types of numbers, say it's probably worth a little bit of effort to write that. So again, the my favorite course, and by the way, there are many providers of these courses because they saw an opportunity to write something fairly consistent and reapply it over and over again, is it bit.ly/ 4557 course on on the grove. Now that one is a very complete course, I did a section of the course. But there were also other well known presenters on that particular topic that were included as well. So among them, and I think you will recognize the names of a number of these people was Don Brolin. And Steve Perkins, who has been a long term client out of Hogan Taylor in Tulsa, and Andrew Lucys, who's the CEO of tech for accountants, well, each of the four of us took a section in that course and tried to explain what to do. But the main point of today is, you need a 4557 written information security plan desperately so you don't fall under the FTC safeguards penalties. Now, there's a lot more we can be talking about will, but Brian did I kind of covered the big issues here.

Brian F. Tankersley, CPA.CITP, CGMA 09:02

So Randy, you know, I, what I would suggest to you here is that if you're looking at this, and you're trying to figure out what the major publications are, there's one more publication that we that we, that we didn't mention that I think is critical to this. And this is just the NIST publication NIS T ir 7621, revision one, Small Business Information Security, the fundamentals. Okay, so you can find that from a quick Google search, but it's a it is kind of the Bible for this. It is 54 pages, and it lists out it's put out but now let me give you some background on news. Okay, NIST is the National Institute of Standards and Technology. So this is a US federal agency that provides standards that the US Federal Government has to has to comply with. However, these standards almost universally, I mean, I've had numerous conversations with pen test urs people to do sock audits Randy and other Kaitou

people and, you know, people from from all across the spectrum. And it seems like everything that shows up in NIST, within five years gets cascaded down to other businesses through regulation. And that's exactly what's happening here. So when you're, when you're doing this plan, this is really the set of standards, that that you're really going to kind of be held to and that you need to think about. So there's just so it's just a nice little publication that you can use. But, you know, again, this is what the, you know, if you're wondering what the real you know, if you're one of these people that digs into the code, and then likes to dig into the rags, and then do ours, think of this as the rags associated with these requirements that are promulgated through here. So this gets down into brass tacks, if you're wondering what you should be doing, because it's a, it's really designed to help you solve that problem. So, you know, if I was if I, you know, I like to print stuff out on paper and read it outside on the porch with my dogs drinking a cup of coffee. And I would suggest to you that this NIST publication and pub 42 557, and pub 5293 would be a great topic for you, when you're fresh in the morning, and you want to kind of digest what these requirements are, you really want to get down to your original sources. So like many of us do.

Randy Johnston 11:32

Yeah, I appreciate that. Now, that NIST document is, again, a brilliant read, like you said, about 54 pages. But it's not trivial reading. Like the other pubs that have called out. There's actually one more pub that I like to cite, which I have, in fact, all of these pubs were Brian and I are talking about, we've read kind of in the end, the pub 1345. Now 1345 is for providers of tax support, and software and so forth. But the reason I call out 1345 is, you know, this protecting taxpayer data is the law. And these online providers have to follow six, security and privacy standards, which include extended validation SSL certificates, they have to do an external vulnerability scan on a weekly basis. They have to follow information privacy and safeguard policies that which are certified by third party, they have to protect against the bulk filing of fraudulent income tax returns, they have to have a public domain registration, and they have to report security incidents as soon as possible. But the piece I'm not sure they can follow is not later than the next business day. Now those six items are all in 1345. And they're kind of like your claim Brian on NIS trickling down. These are pretty good practices to trickle down. And it leads to even more with the security six. Now, many have spoken about the security six, which includes having malware Endpoint Protection response, having firewalls, strong passwords with MFA, and backing up your data and drive encryption, and so forth. We've talked about those on prior Technology Labs. But there are things around mobile devices and wireless kyknet

connectivity that come into play. Further. Part of the reason I personally am so adamant that CPA firms subscribe to at least Microsoft 365 Business Premium, is you get the Advanced Threat Protection and data loss prevention capabilities. And the DLP data loss prevention that you can turn on inside Microsoft 365 helps with 4557 compliance. And there are 10 policies that I like to implement as DLP policies in Business Premium. So you can hear all of a sudden this podcast where we usually focus on a single topic, which we aren't really, it's 4557. And you need to have a written information security plan in place to comply with the FTC safeguard rule. And you gotta find a source. So if you're looking for guidance that I think is good, again, the best course that I've seen published is the groves course, really highly rated. Again, that was at Bitly slash 4557. course now I can tell you, our K two team had written a course, it's probably part of the reason we were lulled into not recording this podcast sooner. Because Brian I taught that course, you know, over the last 18 months or more, and repeatedly have taught that and we just assumed that people were looking at the 1230 One deadline and saying, Yeah, okay, we've got one we'll get we'll get it written. And that didn't happen is the best we can learn because there was misinformation about all firms, everybody who has a p 10, needing a written information security plan. So Brian, I went off on a long rant there, but you kind of get this this this is near and dear to the heart. It's the reason I put in the effort last year and this year, what else is important for our listeners to know?

Brian F. Tankersley, CPA.CITP, CGMA 15:28

Well, I think it's important to note that there is some discussion at the legislative level, it's the federal government about having some kind of privacy regulation put in place. There was actually a a group of left leaning senators that came out with some sort of press release earlier this year saying that they had caught and I'm gonna put that in air quotes. They had caught Tax Act and Sales Tax Act, and it was tax Slayer and h&r Block using Google Analytics. And evidently, using Google Analytics and a Facebook, a Facebook tracking tool, evidently could leak financial information to to Facebook and Google. Now, as an aside, it strikes it strikes me as as odd that everybody seems to get killed, get crucified for leaking data to Facebook and Google, but Google and Facebook never seem to get in trouble for being the conduit through which this data is leaked. But I digress here. The point here is that it's very clear that some some politicians are probably looking to make examples of people similar to the way they made examples of these tax prep firms. And there may be other agendas that foot you know, I know that these these senators are also in favor of having IRS prepare a lot of the tax returns through something to replace refile. But nonetheless, this is something where you don't want to be caught flat footed. And, and again, the

the work that it's required now that they've published a lot of the work from the senator, the record, this required to make an example out of somebody is pretty trivial, honest. So what I would just suggest that you need to do is just be very careful when you get planned together. Because you don't know when you're going to become the target of, you know, you don't know when things are gonna go sideways, and you're gonna, you're gonna be standing there having to explain yourself.

Randy Johnston 17:39

Yeah. So you know, I have one more piece of guidance, and another IRS Form to mention, one of the pieces of guidance throughout all this material is that you should monitor your IEF NS and P tins. And, you know, for Ethan exes, as you know, you can go into your E services account, and select the refund status. And what you're really watching for is, you need to contact the IRS helpdesk if your return totals exceed the number of returns you filed. And for p 10. You can access your online p 10. account and view the returns filed for p 10. And if you've got differences in these numbers than what's expected, you're supposed to complete 14 157, which is the complaint from a tax return prepared report the excessive use or misuse of a p 10. So you know, in this particular case, the monitoring of E fins and P tins you're probably already doing in your firm. But it is supposed to be done on a weekly basis, according to the regulations here. And what we're they're really trying to do is they're trying to spot data theft with these e fin and p 10. abuses. One other final thing that I was pretty adamant with my clients during the past few years, is to make sure that your central centralized authorization file your caf number is up to date, and that you withdraw any authorizations for those who are no longer clients. So Brian, as we're talking about all these things, there are so many little nuances. These are covered in the pubs if you just read the doggone stuff, but the problem is it feels like an onerous task. And our job here on the technology lab is to give you the guidance to make your your jobs easier. And realistically what we're asking you to do I think is the easiest path forward. So Brian, other questions comments that we should ask our users or ask them to ask themselves?

Brian F. Tankersley, CPA.CITP, CGMA 19:46

You know, the thing I would suggest is that is that it is time if you're working off of a a home router without at your office without a plan and you don't really Have you have Griese home? Great antivirus setup is any virus that reports to your managed service provider, somebody said, it's just time for it. Doris is really mandating that you have to grow up from a technology perspective, you don't have to act like an

enterprise where everything is controlled 15 ways to Sunday, but you have to make some steps forward. And so these, these give you the guidelines of what what they want you to do, that give you the guidelines about what you have to do. And just trust me having having helped some people who have been through situations where, where there systems have failed, you know, you don't want to be on the other side, you're going to be you know, you hear a lot about people being on the wrong side of history. You know, you don't want to be a foot you don't want your your your firm to be a footnote in a in a publication about what could go wrong to accounting firms. So I hope you'll hope you'll check that out. You know, I think the the course at the grove is very good. Again, it's a bit.li/ 4557 course, I have no interest in that course. But I've seen it and it's it's good stuff. And I hope you will hope you will consider checking it out if you're not sure which.

Randy Johnston 21:17 Yeah, I appreciate that. You know, I think back in our K to safeguarding taxpayer data course, a guide for your required security plan. We wrote that, you know, almost two years ago, I thought it was fascinating how much focus we had around protecting data and risk. And we identified those 12 steps in Irish pub 4557. So I think for us to close up today. 4557 asked you to do these 12 things, take basic security steps, use security software, create strong passwords, secure wireless networks, protects toward client data, Spot data theft, monitor your events, and P 10s. Recognize phishing scams guard against phishing emails, be safe on the internet, report data loss the IRS and state authorities and respond and recover from a data loss. And there are many items that have to be done for you to be able to do that. So this is a big deal. And again, we should have probably recorded this as a session sooner rather than later. But when we were looking at our catalog, we realized you know, we don't have direct 4557 guidance in the technology lab. And you as our listeners need to know that. So we appreciate your time again today. And we hope you already have a written information security plan in in the plan done and in the can. But maybe you picked up a new idea for perhaps for example, applying data loss prevention policies might be another example. So we appreciate your time and we look forward to having you join us on another technol

Accounting • Firm Management • Security • Technology