We are now to the portion of our program where we're going to talk about data security issues. In today's world, it seems like there's not much out there that you can't find out about anyone on the internet. Because of this, much has changed about the practice of law, especially in the field of protecting information. We are used to it from the very beginning of the notion of attorney-client confidentiality; however, some of you may not be aware that there are a myriad of ways that we can get ourselves into trouble having to do with the storage of data, including names, addresses, Social Security numbers and dates of birth. As you all know, I represent subsidized management companies. In my files, I could create identities for about 2,000 people because I have birth dates. I have names of children. I have mother's maiden names because that's what they're required to do. So I have to start thinking about that. You know, in the old days, it was, like, heh, who's going to come and, you know, steal these files? But now, more and more, there's more security breaches to do that. So here to let us know about what are obligations, I'm going to present somebody who spends a lot of time thinking about these kind of obligations and things that need to happen. And once - he'd like to give you some of his ideas about what you can do to protect yourself. I have Matthew Pettine. He possesses over 30 years of diverse experience combined with highly technical knowledge and ability. Now, you all know I have been spending two days doing alphabet soup. His is one of the worst ones, so just bear with me. His discipline approach to organizations an IT development complements his ability to anticipate potential obstacles. He fully understands business and unappreciates how different functions interrelate. He understands, also, the nuances of a diverse workforce, uses technology to compete in today's business world. These attributes contribute to his strong record of excellence and successful delivery of bottom-line solutions that positively impact the bottom line of a company. His industry experience includes management positions, providing technical and managerial consulting, business risk assessment - jeez, what a fun gig that is - customized applications developed in - and infrastructure solutions. He has his bachelor of science in business administration and management from Northeastern University and completed his MBA at Southern New Hampshire University. So Matt, take it away.

>>: Woohoo, thank you. Let's see. All right, there's a couple slides about me, about my firm. The gist of it is I'm actually an IT auditor. So I'm not just an IT auditor but I work for a large CPA and consulting firm, so I'm also a client of quite a few of these regulations. So I'm responsible for doing it for us, and then companies' clients will have us come in and help advise them, typically kind of larger companies. We have all sorts of services at MFA. Enough said about that. And there are just so many privacy and electronic data regulations these days. Depending on the industry, the type of data that you deal with, you know, I would be surprised if anyone could not be in scope with at least a few of them, in particular

in Massachusetts. And I'll get more into the Mass. regulations. Anyone doing business with people has obligations to keep the data safe. So I'll get a little bit into the specifics. I typically speak after attorneys and the attorneys talk about all the breach cases and they scare you with penalties and things, and then you guys, like, listen to every word that I say because I tell you how to avoid all that. A couple of them that are up here, you've probably heard the acronyms HIPAA has to do with health care. HITECh is just some more detail around that. There's certainly a ton that have to do with financial services. Anybody that's taking credit card information, there's a whole line on that, certainly anyone doing real estate or anyone with private personal information. And there are even rules about sending spam, which you'd be surprised because I'm sure you all get tons of it. But as legitimate businesses, there are do's and don'ts for what you can do for unsolicited marketing materials. Luckily...

>>: That's a nicer way of calling it spam - unsolicited...

>>: Isn't it?

>>: ...Marketing material.

>>: You know, I used to know what spam stood for. It stands for something. Do you remember what it...

>>: I don't know.

>>: You're talking about the old radio or are you talking about...

>>: No, spam.

>>: Like the meat?

>>: When you refer to it with email, it's...

>>: It's got to come out of the military, I would think. I'll look it up.

>>: I think it's...

>>: Talk amongst yourselves.

>>: I think it's an acronym. We're all computer people up here.

>>: I'm not, but OK, I'll look it up.

>>: The good news about most of these, and especially from a technological perspective, no matter what the data is, what you're trying to protect, what you're trying to keep people into, most of the controls are the same. It's sitting on your computer. You're sending it through email. So all of these regulations, the specifics can be different, but they all require, you know, physical, technical and administrative controls. And I'll explain what that means. They're all concerned with protection against unauthorized access or disclosure.

>>: It's from Monty Python.

>>: What's that?

>>: The spam. It's meant to - an irritating, large, meaningless block of text. In this way, it was called spamming. Because if you remember the thing where they all talk about SPAM, SPAM, SPAM, SPAM, SPAM.

>>: Oh, I think someone made it up a...

>>: Thank you, Monty Python.

>>: ...Four-word...

>>: Oh, I'll look at - I'll keep going.

>>: ...That matched it, but I believe you.

>>: All of the regulations have notification requirements. So if it does happen, there are requirements for you to tell either the people involved or some regulatory body. They all require written policies, which sometimes is difficult for smaller companies. It's not difficult, but it's less common. If you're a sole proprietor, in my experience, you're very unlikely to actually write your own security policy because it's you. Regardless, you probably want to pen something together just to have it in case someone ever asked you for it. Most of them require training. And as a practical matter, training is maybe one of the most important controls you can have to avoid this. Part of it is what you're getting here, and I'll talk more about that. And especially for larger organizations, there's an emphasis on your processes being repeatable. Again, for a smaller company, I'm not sure. I mean, you probably do your own work the same way every time. Once you're large enough, if you ever get there and you have 100 people, you might want to have written standard operating procedures. Then at the bottom, it said enforcement and penalties. So if you do stuff wrong, all sorts of bad things happen to you. I tend to pick, in this

presentation, 201 CMR 17.00, which is the Massachusetts privacy regulation. It's got a lot of specific pieces in it, and it's general enough that it applies to most industries, most practice areas, most pieces of information. So the intent of the Massachusetts regulation is to prevent personal information from being breached in the first place. When it came out, it was unique in that regard. So there were tons of regulations that told you what you had to do after a breach. You know, and the penalties and what you had done wrong, Massachusetts actually wanted this put in place for all the businesses before anything ever happened. And the idea was they were going to try to prevent it, which was a good idea. There was - I went to some of the public hearings for it, and it was interesting because there was one group that said this just goes too far - a lot of techie people - you can't tell us what we need to do, it's too specific. And then there was another group that just, you know, no one's doing anything, we need to put teeth in it, and we need to have people actually pay attention. And of course, it has minimum standards and responsibilities and reporting protocols. It's not unique anymore that it kind of prescribes what you need to do. Several other states have it. Several other, you know, regulatory bodies are either describing what you need to do or there have been judgments and decisions and guidance that tell you what you need to do. So we'll go through that stuff. Massachusetts, in particular, cares about people, cares about citizens. And what they focus on - the data that's in scope for this regulation is a person's first and last name or their first initial and their last name combined with something that could cause that person harm if it were lost, so a credit card number, a Social Security number, any sort of financial account number, anything that's not public and can cause them damage. So one of my examples I use is a personal check. If you get a personal check from someone, you have their name and their bank account number. That's in scope. If you lose it, you just had a breach. Depending on what it is for the other regulations, other things are in scope. Some other - Massachusetts only cares about Massachusetts which is fascinating. So even if you're a New Hampshire firm, if you're dealing with a Massachusetts' client, technically you're in scope for this, and they say they've got jurisdiction because they're protecting the people. But other states have different requirements. Massachusetts is kind of simple where it's just - it's the name and this information. Some states worry about date of birth. They worry about email addresses. In general, especially for smaller groups, we just recommend people keep all their confidential information confidential. You're not going to put your list of names and Social Security numbers on a different server than everything else that you're holding. So if you just apply these controls to your computer, to your data files, you should be safe, and you should keep it all - where this comes into play is if something actually gets lost, then you want to figure out exactly what it is and minimize the scope as much as possible. Makes sense. I'm looking at people nodding. I mentioned it's very widely applicable. So when they were going through the hearings, they kept rewording it to get rid

of loopholes. So you know, I hold the data, but I don't actually own it. I'm a steward for it, and then they'd put a little blurb in. So I forget what the final sentence was, but it's this long sentence about anybody that owns, receives, stores, manipulates, communicates. So basically, if you have an opportunity to lose someone's data, it applies to you. Also, if there were some sort of action taken, there are some things you can do for vendor management. But anybody in the whole chain is really subject to scrutiny. So if you take it but you put it on a cloud service, and then something else happens with it, really, they can pick on everybody for the whole chain. The best case - the best you can do for protecting yourselves for some of those services is to really just do good due diligence, make sure you're comfortable with them and then have some proof of it afterwards. If you are holding stuff on some unnamed cloud service and they have a breach, you want to show that you did everything you could, and it's really their fault. It's not your fault for picking them. Make sense? Am I talking really fast?

>>: You got a question.

>>: Sure.

>>: So for example, like, if you use Google Drive and you set up a password and this is the third-step verification of the log-in where you get, like, a code, you know, so you set up all those protections, but then there's a Google breach. Is that enough - did you take enough steps then to protect that information or...

>>: So this is all my opinion - probably not.

>>: You need to repeat the question.

>>: Oh, so the question was if you were to use Google Drive, and you do everything appropriately for what Google Drive's consumer service tells you to do - you've got passwords and everything - but Google loses the information somehow. Could that come back at you? And I would say, yes. And even reading some of your text - and the Massachusetts's regulation is, like, three pages long. But there are some other pieces that Massachusetts and the other bodies would want you to do. And I'll kind of get into it. And I'll try to use - I tried to avoid using vendor names when I'm saying anything negative, but...

>>: And here's a question though because I've never tried it.

>>: Sure.

>>: Maybe you have. Can you encrypt something on Google Drive?

>>: So Google and a lot of the cloud services have two different versions, which is very applicable to this audience. They have consumer services, and they have business services. And the business services might be too expensive for anybody starting out, and the consumer services do not. So they do something called obfuscating. So they take a piece of paper, and they rip it up, and they put the pieces out of order, but they don't actually encrypt it, which means you can't read it. So somebody else with a computer that has, you know, a puzzle program can put it back together. So technically, it doesn't count as being encrypted. There are some other issues with some of the computer services that apply to privacy regulations. Every time you use anything, it says click here to accept the terms and conditions. If you're using it for anything confidential, please read the terms and conditions, even though they're five pages of just painful to read through. Many of them, you're giving them a license to whatever you're putting on there. You're giving them your IP, you're giving - if it's associated with a common search engine that I know, any of the services that you use from that unnamed common search engine, including translation. So my firm wanted to use them to translate documents from our Canadian office from French to English. You give them a perpetual license to that information. And it is probably unlikely that that contract would show up in a Google search, but it might not be unlikely if someone were searching for, you know, sale of a public company related to biotech. For something about that to come up and that would be our fault. And unless you read it, you have no idea because you're just putting something in a webpage and getting it back in French. There are some free radio apps out there. And if you don't read it, you don't realize that you're giving them a license to your network, your storage and your processing. So some of these cloud services, the real legitimate ones that have their own servers in a big bank somewhere on Amazon, they run their own equipment. Some of them are peer to peer. So what it means is their entire service runs off their clients' computers. So Brian might be listening to a song that happens to be on Catherine's computer because that service...

>>: You're welcome.

>>: ...Decided Catherine had the best bandwidth of everybody in the area. And we had users in my office, MFA in Tewksbury, suddenly our firewall traffic was going crazy. We have a really good connection, so this particular music application said, they have a really good connection, and they put all of the music on this guy's, and he was farming it out to everybody else, which in privacy terms, your letting - oh, sorry people online - you're letting people into your network that you don't know, you don't have control over. And I haven't heard of breaches resulting from that, but you can't let people into your network, so. Yeah, it's horrible. Go ahead.

>>: So you're completely terrifying us.

>>: Excellent.

>>: What do you do if you don't like the terms and conditions of a product that you want to use?

>>: You do not use it.

>>: You have to find an alternative.

>>: Yup.

>>: And it's - you know, the one thing going back to your question, you have to keep in mind these raised regulations come from. They're not the attorney-protection regulation. This all came out of, you know, TJX losing, you know, access. This is to protect the consumer, so it's going to be geared to that. So it's sort of like you remember Terry yesterday talking about, you know, you may not end up ultimately being liable, but you're damn well going to get sued. Why? Because you're presumed to have the deeper pocket that somebody else doesn't have, particularly some kind of company that's not really based here in Massachusetts. Well, guess what? You are. So you need to start thinking about that is that, you know, the fact is you cannot necessarily just say, well, I relied upon somebody who told me that they were going do it. They're going to ask you questions like did you read that contract? And if you're like me, I don't read those damn things because I fall asleep reading them. Sorry...

>>: Absolutely.

>>: ...You know.

>>: So I'm going to rush forward because we have a bunch of slides, but I am here for the question part right before lunch because I thought it was at, like, 4:30.

>>: Nope.

>>: All right.

>>: I don't torment the techies that much.

>>: And I'm also going to go fast enough that you guys are going to go, like, what, what, what? So if you start to look really confused, I'll slow down. But some of it, I want to give you the background, but there's really like two sentences and most of them showed up on Brian's slide about security. So failure

to comply, I don't have to say a ton about this. You can get to sued. You can get in trouble with criminal penalties. Different regulatory bodies can do different things to you. If you're big and you have the FTC come in, then you're just in a world of hurt for years and years and years. Beyond that - and most companies don't worry so much about the fine as the reputational problem. Company - you know, attorneys, if you are in the newspaper, if you have a very public breach, you know, it's not good for your business. And it's very specific what you have to do. If you lose two people for at least Massachusetts and you know who they are, you can go communicate with them. If you can't say exactly whose information was lost or it's an awful lot of people, there's alternative notification which literally means taking out ads in newspapers saying we lost your data. If, you know, if you were involved in this, let us know. You also need a good attorney, someone that's familiar with these regulations if something were to happen because the different regulations - and you could have one breach if you deal with people in different states, and you could be - you could have to respond to several different states. And the responses are different. Massachusetts doesn't want you putting details in. It had to do with the Boston Globe, and they put the details out, and then hackers went out the next day and found - they put a map of where all the credit cards went, and they found the ones that were left. So Massachusetts doesn't want too much detail. Other states, other jurisdictions want it in, you know, excruciating pain. So we don't not want to comply. And not complying is not the same as having a breach. So not complying means you didn't do the steps that we're talking about, the protections that you put in place. Nothing's 100 percent. It's understood that something could possibly happen. You just want to prove that you weren't negligent, that it wasn't a breach of contract with your clients, that you did all that you could do reasonably. So there are six general steps. The first is to do a risk assessment. So what that means is just understanding the information that you are holding, where it is, what you're doing with it, where it goes - obviously, much easier for a smaller firm than a bigger firm. Once you know what you've got, you identify what the risks are. And that's really - we call it a what-could-go-wrong list. I could lose my laptop, you know. Someone could physically break into my office and steal my files. You think of all the things that reasonably could go wrong, and you note those down. And then you evaluate control. So a control is just something that you've got in place to help mitigate that risk. I could lose my laptop, but my laptop is encrypted, so it's no longer a breach. Someone could break into my office. Well, I've got locks on the door, I've got passwords on my computer, my file cabinet is locked. Iot. Things like that. And then at the bottom, you figure out any place where you've got risks and you haven't done something to address them. So I carry my laptop around. It's not encrypted. What do I do? I encrypt it. So it's really, you know, it's meant to give you a sense and something that Catherine had said when this came out part of the concept for 201 CMR 17.00 was that the people running the business could no longer turn to their

IT people and say I didn't know. They couldn't get away with just pleading ignorance, so that's no longer a defense for this stuff. The idea, especially from the risk assessment, is that management understands what the risks are. They may not - you might not understand in detail what all the controls are, but you're responsible for it. You have to designate a security coordinator. It will likely be you if you're starting.

>>: You wait till you have those meetings with yourself to talk about all your concerns about what you're doing.

>>: So you may want advisers, but you are responsible. You're the security coordinator. You want to document the information flows, the controls, the policies. Like I said, you won't have a lot of policy. For 201 CMR 17.00 and for a lot of the other ones, they do want a written security policy. They'll call it a WISP. Other ones will call it something else. Massachusetts, the Office of Consumer Affairs and Business Regulation had some samples, which are kind of half fill in the blank, half please put what you do here. You wind up with, like, a three- or four-page document. Even if it's just you, it's not a bad idea to do that, to have it in place. And depending on who your clients are, we're seeing a lot of banks, a lot of financial institutions, requesting something from their business associates before they do business with them. So you may want to even paraphrase that into a little marketing spin of this is how we keep your information secure. And then when someone requests it, you're comfortable giving it to them. I would caution you, don't put too much detail into something that you're going to share with people. Don't say I have a Meraki 752 firewall that's plugged in, and we let these two ports in.

>>: And if you look up here, it tells you how to get around it.

>>: Exactly. You know, and develop employee consequences for non-adherence. So if you don't have employees, it doesn't matter. If you do, 99 percent of the time it's a sentence at the bottom of the policy that says, you know, failure to comply could result in consequences up to and including being let go...

>>: Termination.

>>: ...Something like that.

>>: Termination. It's like the side effects of all those drugs...

>>: Yeah.

>>: ...You know.

>>: Yeah, a lot of them. No, it's much shorter. It's one sentence. So in the Massachusetts regulation, which was one of the reasons that everybody got so interested in it, they actually have eight bullet points of areas that you need to do. Like I said, a lot of the other regulatory bodies have jumped on and done the same thing. But at the time, we were like, whoa, what are lawyers and politicians telling us to do with our IT stuff? Authentication means logging in. It means telling your computer who's using it. So you have to have control of - you have to have a password. You have to have control of the IDs. The passwords have to be reasonably secure. So these days that means, complex is what they call it. And there's usually a checkbox on a Windows machine that use complex password, but it's an upper case, a lowercase, a number, a symbol, something like that. You should have them expire. And it's actually more important than you might think because over time, there's more and more chance that somebody either learns your password, somebody malicious out on the internet gets your password. Yahoo has a hack, you know, five years ago, and you haven't changed your password since, and you're using the same password so some guy has got it. And you should block access after multiple attempts. So as the business owner, all of these are kind of settings that you can set on your computer as you go through to enforce it. If you're a sole proprietor, just make sure you do this. You don't even have to enforce it. If you've got employees or you share your network with people, as much as you can, make these computer settings. As an auditor, you might do it, but you can't prove it to me unless I see the checkbox on the computer. So if I come afterwards to see if you've really got complex passwords, you might, but if the checkbox isn't checked off, I have no assurance that you absolutely do. Does that make sense?

>>: So where are those - where does the checkboxes pop up? Like, where are they - is it when you install it? Or is it...

>>: No, you kind of got to get a little bit into it.

>>: OK.

>>: So it's in the settings, typically in the registry. Or if you have a Microsoft network, Google it or YouTube it - how to set up the policy because they change it with every version. And the versions are changing every 18 months these days. So but once you get to it, it's a checkbox, and you can just check it off.

>>: What is happening? What (unintelligible)?

>>: So it's setting it for complex passwords, setting it so your password is enforced to expire after 90 days, setting it so it locks people out if you put your password in wrong three times, seven times, 10 times. All of those things help keep your computer safe from other people getting into them. The next one is kind of related to authentication. So authentication, you tell the computer who you are. Access controls, you tell the computer who gets access to what. So the best practice is called least privilege. So you only have access to the data that you need to do your job. Massachusetts and the other regulatory bodies tell you you have to do this. If you're a small firm, it may not be as applicable. But even if you've only got two or three people, I think you can appreciate you don't want the receptionist to be able to get to the payroll system. So if you keep that in mind, that's the viewpoint that Massachusetts is taking towards private information. You don't need some office worker to be able to get into the guts of your file. If they do, if you're small enough, and they're your assistant, and they have a reason to be there, that's fine. You know, that's a need to know. They're using it for their business. But the guy that waters the plants absolutely can't get to, you know, the Social Security numbers of your client. All of the computer systems have ways to determine who has permissions to what, even the cloud systems. And again, you right-click, you say policies. It's only applicable if you have more than one user. If it's just you and it's just your laptop, it just doesn't matter. If you're sharing information on a server between people, then it does. IDs - I'm editing myself. Attached to this one is the one that says not vendor-supplied defaults that I know Brian mentioned earlier. Everything you do, make sure you change the password, so not only when you buy the router, but when you sign up for paychecks for your one employee and they give you a login. And specifically, it's in quotes because it's in the regulation. So make sure you change all of your passwords when you have a service or a device from the vendor's supply - supply default because it's just so easy. So many people got hacked. Making sense? Beyond that, once you get much bigger, come see another seminar where we're speaking for bigger companies, and I can get deeper into it. There's two pieces about encryption. One is encryption at rest, which I'll talk about in a little bit and in data transmission. So the regulations say things have to be encrypted when they're communicated where technically feasible. I always get the question and the one spot that there was some guidance that it wasn't generally technically feasible was faxes. So over the public switched telephone network, right now, you don't have to put any extra device on to encrypt your fax. You should make sure that your incoming faxes go to a place where the people who might see them are able to see them. And you should make sure that if you're faxing to someone, and it's got personal information, that it's going to a private fax machine, or you've warned them and they're waiting for it. But beyond that, it's technically feasible to encrypt pretty much any digital communication at this point. Email sometimes is a little trickier. And most often, you just get a service. So your email service may have, you know, type secure,

and we'll make it encrypted, or pay $10 more and we'll do it. It's an extra step. So for you it tends not to be - for the sender it tends not to be that difficult. It's something like a keyword in the subject. For the receiver, instead of getting your email, I get an email telling me you sent me something with the link in it. Then, I click on the link and I have to, you know, set up a name and a password and be able to get into it. But it keeps it encrypted. And it's much easier than it was 10 years ago where you had to have like two IT people on either end talk to each other. And then, we'd pass the person the note. Remote access, any of the online services - if you're bigger and you're dealing with benefit plans, you know, don't email Excel files with all your employees and their dates of hire and their Social Security numbers. Wireless, all data - so everything else we're talking about communicating personal information. And then, in this same regulation, it says wireless data must be encrypted, all wireless data. The reason being, if you don't have encryption on your Wi-Fi points, then someone can get on your network and kind of bypass your firewall, bypass a lot of the other controls you've got in place. It would be difficult today to set up a wireless network without having it encrypted, honestly. So if you do just buy it and plug it in, you're probably safe. But you want to make sure. You want to double check. And you want to make sure you put passwords on it all. There's an element of monitoring and that and risk management, risk assessment, have a lot of emphasis on a lot of the regulations, currently. So there's a renewed emphasis. There's been some changes in COSO, which does auditing standards. It would be difficult for sole proprietors or two or three-person shops to adequately monitor their own - you know, you're not going to look at your firewall logs. You're not going to know what it means. Many of the systems that you're getting - so if you set up a backup system or an anti-virus system or a secure email system, they kind of monitor themselves. And they send you an email if something is off. So that can probably suffice for the smaller firms that if something happens, it alerts you. And you kind of pay attention to those alerts. Once you get bigger, you actually have to have people looking through these things and analyzing them and spending lots of money. Big companies spend a lot of money to do this stuff. You know, if you're targeted after you went through that breach, today, they can tell you, like, where every packet goes in every network. So you don't have to worry about monitoring too much. You do have to worry about encryption of personal devices. I love it because now if the information - if your entire laptop is encrypted and you lose it - at least for Massachusetts and for most others - it's not a breach because they don't have access to the information. There are third-party tools that are very common. They're like $100. You put it on. It encrypts your drive, and you never have to worry about it. Some of the newer computers themselves do it, just as part of the computer. So you just look into - most of them will say something about computer security. And if you just read the fine print, it'll say if it's encrypted or not. And if not, buy something. But it does - it gives you a lot of peace of mind. It's kind of a pain to have to

remember and then to do it. But once you've done it, you know, you're not losing your private information, your home pictures aren't showing up on somebody else's Facebook page.

>>: (Laughter).

>>: There's all sorts of good reasons. What you also have to keep in mind is it's talking about any portable devices. So those little USB drives are much harder to encrypt. But if you use them and you've got confidential information, you're in violation of it. You can encrypt them but you're better off finding an alternate means of getting people things. Backup media - if you backup to tapes, the tapes have to be encrypted, which generally means that - most of the software does it today. You just have to take the extra step of putting the password on, and it encrypts it. Phones - so if you sync your phone with your email by some service and you communicate via email and have personal information in the communication, you should have your phone encrypted. Most of the phones will encrypt if you've turned on the password. So I have an iPhone. If I don't have a password, it's not encrypted. If I put a password on it, it suddenly encrypts everything so people can't steal it and try to get the information. So encryption is awesome. It's your friend. We talked about firewalls. There are a couple of specific pieces in the regulations that talk about the firewall being vendor-supported, reasonably up to date, that your operating system has to be patched. For most computers, they're going to apply their own security patches unless you tell it not to. So the guidance is don't tell it not to. Tell it yes, I accept your security patches, thank you. For the firewalls, for anti-virus systems, it gets a little more complicated. It used to be you could buy a firewall and you'd own it for like 10 years. And you'd get the maintenance, and every once in a while you'd have to run some program that would update it. It's still not too bad with the consumer product. But as you get higher up, the vendors will just stop supporting them. So for our company, once my firewall hits about 3 years old - and we've got a big Cisco one - we just can't even use it anymore. It's still doing exactly what it's been doing, but it's not up to snuff for the current - the risks to computers are moving so quickly that this is how the industry has gone. That it's every few years you need to do something with it. In your case, practically, you're probably safe because in my experience, the little wireless firewall routers that we purchase last about two or three years at best. And then, the radio starts going and you go to Best Buy, and you buy a new one anyway. You need anti-virus software. And I could tell you all sorts of stories about, you know, we turned a computer on, started - plugged it in and started to install the AV. And it had a virus before the anti-virus software got on there within like 10 minutes of being plugged into the Internet. It's unbelievable. So make sure you have anti-virus. Make sure you educate and train your employees and yourselves, you know, there are all sorts of webinars, seminars. There are probably trade magazines for the legal profession that have articles about it. You

know, Brian's right about the phishing, the ransomware. People are the weak link or tend to be the weak link. And you just have to - you have to be aware of what's happening that the IRS is not sending you your W-2 as a Word document and wanting you to open it. But they're getting really interesting about how they can impact you. You don't have to be as stupid as you used to have to be. You can be fairly intelligent and still get pulled in. And it's not necessarily going in - and it's not just necessarily going and giving them your name and password. In some cases, it's just going to their website. It's just clicking on the link at all. In some cases, depending on how good they are, it's just seeing the preview of the email can run some stuff. It's really scary. I see the really good ones. Luckily, no one is really targeting you as bad as they are some of those other companies. But going to assessing third-party vendors, they may target you if you have a client that they want to target. So they got into Target through the HVAC vendor. And just on and on, all of the stories come out that the bigger companies have really good protections. All those eight bullet points I talked about. But the people that they let in don't necessarily. So this applies for you folks when you're using the online Google Docs service. You have to be - you have to do due diligence. You have to be comfortable that the people that you're sharing information with can hold it secure. So when Stephanie was saying cheapest isn't always better, especially for any services that you're putting private information out. You want to see that they've got some sort of report - And I think I'm on my last slide so I'll take my extra minute - that they have some sort of report that - they give you some sort of assurance. Most of them will have some sort of sheet of paper that you can look up online that says what they do for security. Your obligation is to somehow document that you've done that due diligence. At MFA, when we deal with vendors, we require them to either give us what they've got - So they've got a (unintelligible) reporter or S70 or some compliance report - or we give them something that they have to sign. And if it's an online service, you know, there's no person I can give it to and get a signature. So we do a lot due diligence. We really look into them deeply. And it's part of the regulation. So the safeguards have to be part of your contract with them. Train your employees. Monitor compliance. We kind of talked about the steps. And I'm done, not too bad.