1:11

Good morning, everyone. Thanks for joining. We're just going to give people another minute or so, and then we will get started.

2:39

All right. Good morning, everyone and thank you so much for joining yield for shield getting compliant by March 2020 few comments before we get started. This webinar is being recorded and you will receive the recording and the slide deck later today and we will have time for Q&A at the end of the presentation. So be sure to put any questions you have throughout the presentation in the chat and we will get those answered.

3:06

And just going to do a quick overview of all of the companies involved in today's webinar.

3:13

So let me tell you about Harris Beach. Harris Beach and its subsidiaries provide a full range of legal and Professional Services for clients across New York State as well as nationally and internationally, we have actually more offices in the state than any other law firm and feature 27 practice groups and represent more than 20 Industries through the Strategic application of our resources relationships legal experience and Consulting expertise.

3:41

We've built the right team to get the job done for our clients both efficiently and more also importantly cost-effectively. So thanks pass it over to Mike. This is Mike Compisi and a little bit about Caetra.io one of the related entities in the Harris Beach family the Caetra.io leverages the legal knowledge of the Harris Beach attorneys and incorporates it into its automated cybersecurity complete cyber compliance platform called cymetric built the help companies manage and be compliant with complicated data privacy and data security regulations cymetric delivers

4:12

Company-specific cybersecurity policy documents along with defined procedures and processes that satisfy one or can consolidate many regulatory mandates while reflecting the risk profile but companies that use it.

4:26

And iV4, we are an IT consulting security cloud and managed Services organization. We are also a recognized as a top Microsoft partner. Our goal is to help our clients do business better by securing and modernizing their it environments. And today. Our presenters are Alan Winchester who is the leader of the cyber security protection and response practice with Harris Beach Michael Campisi who's the president and general manager at

4:55

Caetra.io and Michael Montagliano who is Chief technology officer at iV4 and with that. I'm going to turn it over to Michael who's going to kick it off with the agenda. Good morning, everyone. And again, thanks for joining us this morning. Really appreciate your attendance. Today we're going to go through the need for shield. Why did The Shield Act of come into being owns going to walk you through the important deadlines and applicability of The Shield act then?

5:25

Back over to me. I'm going to talk a little bit about system categorization and boundaries. So we want to put a little bit of context around the shield act and give you some things to consider as you start to think about the legislation and the regulatory requirements will go into the shield act details will talk about security program considerations developing managing and monitoring controls and then we'll finish with some QA.

5:52

So the need for shield the question is why didn't York State go that we needed another piece of regulatory legislation. It feels like every other day another piece of Regulatory Compliance comes out. And so what we like to do is begin every presentation by setting the table and explaining a little bit of what our perception is of the the reasoning behind the shield back.

6:22

So it starts there's there's two components in the legislation itself. There's a purpose and a justification section within the app itself as we read through that just pluck the couple of lines out of the of the legislation itself. First the purpose which states New York State's data breach notification law needs to be updated to keep Pace with current technology.

6:47

So if we look at the current technology Stacks out there, it's really easily understood why the state felt they needed to enable this law over the past several years organizations have been going through a digital transformation as they move workloads from on-premise to multiple platforms, whether software platform infrastructure-as-a-service. The data stack is moving. That is the New Frontier. Used to be in the old days. You could put a moat around your data.

7:17

Today data is now moved on to multiple platforms which increases the attack surface, it's broadened. So they containment and control of that information has become much more difficult.

7:30

The second component is the threat landscape has changed. Attackers are taking advantage of new types of tools like artificial intelligence machine learning big data analytics and they're taking these tools and they lead into capabilities like shapeshifter malware for instance, which has the ability to analyze the environment that it's in and modify its code on the Fly.

7:55

Other things like search engine optimization account takeover attacks. These are new types of attacks that are on the rise and lastly cybercrime economics. It's staggering to think that by 2021 there will be six trillion dollars of global losses per year due to cyber crime activity for the state what that means.

8:21

Is that the cost from 2018-2019 rose to a hundred and forty eight dollars per record Lost and the average cost of a breach now stands at three point eight six million dollars. So three compelling reasons organizations are changing their their environments. The threat landscapeis has changed metabolic vulnerabilities of gone up three hundred forty two percent in the last four years and it's big business. A lot of money is being made by cyber criminal organizations. It's a 5 to 1.

8:55

Ratio cybercrime over all of the security companies that are trying to prevent cyber crime. So the purpose in the new Shield Act is pretty evident. The other component that I pulled out was the justification and I'm just going to address the top portion of this that York State also needs to join the increasing number of states that require reasonable data security protections, but without imposing duplicate applications, and we'll address we'll talk a little bit about without imposing.

9:25

caution small business a little bit later in the presentation, but if you look at the the Slide you'll see on the right-hand side in 2016. The number of states that had data security laws in place and in 2018, you can see just in the graphics the change that occurred that in 2019 25 additional states have laws that address data security practices and in August the least an database showed hundreds of bills that covered all 50 states the territories the District of Columbia.

10:02

Put it out quoting me to a site this morning that shows that all 50 states now have some form of breach notification center security and privacy laws in place. So let's move into the shield a cassette. We're going to turn things over to Alan.

10:16

So good morning. I'm Alan Winchester. I'm with Harris Beach and super excited to be here in super glad you're giving us an hour of your time to listen to this. So thank you very much. The shield Act was sort of came in two parts. Right one is passed the October requirements, but that didn't ask a lot of the organization's to which it applies.

10:43

What it did is the expanded what you already had to do Under the existing Shield law to cover some additional types of Data, and the ones that added was biometric data and for people that don't know biometric data is like the digitization of your fingerprint or an eye scanner the face thing that you see like, you know, your iPhone you lift it up and it recognizes your face and let you do stuff.

11:05

Right that is fire metric information about you that if it got out would allow someone to theoretically use that information to log into other information, you know other sites that has biometric information I so it's a very very personal type of data that could tell a lot about Out you it also extended it to it did already have financial information coupled with a password. So if for some reason someone were to get like your bank account password and the end and the account name and login that certainly would have required of notification under the Old Law under the new law.

11:40

They've expanded that broader so that if you have a say a bank account number, but they also have things like, you know, your mother's maiden name or information about your Family enough that you could socially engineer someone at a financial institution or credit card or something to give them access to your account. You know with the last track not electric like a soundtrack of a crying baby in the background someone seeing like super stress, right that often gets people who are in the service business to help you can trick people into doing things. So now financial information where the other information email account information and passwords is another thing that's now included in it.

12:17

So, it's not just my email address if Email address gets out there that does not that's not enough. It needs to be my email address plus the password to get into it. So you're actually getting to the content by email. We also see that the law expanded the definition of what a breaches it increase the fines double them more than double Dome actually from what they were. So that's the part that's passed but from you know, the activities that you and the audience need to worry about really it's just change your Disaster Response plans to include the additional categories of data.

12:49

So that you act as you had to do Under the Old Law with additional sources of data, so that's that's something that you have to do, but it's not a big big list a big lift comes in the March 20 20, March 23 to be precise. Although probably if you wait till then is it's going to be problematic. But but sometime between now and March 23, you need to implement reasonable and they have two different categories depending on who you are technical administrative.

13:19

And physical safeguards to protect your information and they also give fines for the failure to do that and injunction capabilities to the attorney general. So that's a that's a big the March 1 is the is the nuclear thing that people need to worry about the October 1 that's passed.

13:36

I don't think there's a huge huge lift for most people to achieve but the March 1 that's going to knock a couple of companies back on their heels because it really has a bit of a big ask So let's let's talk about the information. You know, we talked about some of the new ones that did the old ones are social security numbers. So if you have you know, my name is social security number. That's that's the problem right if that gets out saying with driver's license or a non-driver identification card is another thing we protect we also are protecting as I said the account numbers and the email and the biometric so that's like super detail for you slide. It's on you can take home you have it.

14:16

That's what we covered before. It has to be unencrypted not publicly available. Right? So if this information were to get out but be encrypted then it's not necessarily A reach because no one actually accessed it because it was protected. But if it's exposed and someone can actually use the information then it then it's a problem. So let's talk about what a breach is because because that change to under under the Old Law a breach was the unauthorized acquisition of private.

14:46

Information the law changed now in addition to acquisition of the data accesses enough.

14:55

So if someone gets to it ability where they can see the information, but they didn't necessarily upload it or they touch the record and had some way to get in you can see that they got to the records and they were unencrypted and they were not protected that's access and access is is a lower standard than acquisition because acquisition you Look at logs and see well nothing was downloaded by this IP address. Therefore. I don't have to worry because they didn't actually get the information. Yeah, they got through my firewall. Yeah, they got to the data. They got into the server they touch the file, but they didn't actually download anything. I don't have to worry. That's no longer the case.

15:34

Now if if there's a reasonable argument to be made that they actually touch the file they accessed it and if they weren't authorized or they weren't allowed to do it then you have to give all notification requirements under the law So turning the controller back so Michael so a couple slides back Alan talked about the new data types that you need to be concerned about. So what we found is our clients really struggle with identifying where regulated data resides and it's much like a where's Waldo exercise.

16:13

I thought the screen was kind of a visual representation of trying to find regulated data amongst all of the data that you Old in your systems that is peppered across multiple systems many of our clients do not have any type of app classification process in place or any automated tools that they can leverage to discover and tag that information. So and the first step in managing data is you have to understand where that data exists and what systems that that is stored on in order to contain arise and manage that data as you can see up in the upper right-hand.

16:51

Hand side statistics show that 41 percent of companies have over a thousand sensitive files including credit card information health records left unprotected. Let me give you a quick story and maybe this will help underscore the point. We had a client that had to size of their manufacturing business one is a defense contractor, obviously fall under DOD regulations, and the other was a commercial segment that did not fall in the dod regulations.

17:20

We were asked to evaluate Waiter current data governance strategy and when we deliver the results and explain the effort in separating DOD information from commercial data, they gave up they just split the company into two separate companies built out to separate data centers and even try to isolate the information was too much of a lip. So it just illustrates the challenge that you're going to go through and identify any tagging all that information to make sure that you can monitor and manage it.

17:50

So I'm going to look at a couple of options in terms of scoping information. And when I say scoping what we're trying to do with regulated data is to isolate it we're trying to reduce the scope of controls that you need to apply and only apply it to regulated information. So I'll by the way for anybody who didn't want to know where Waldo was look away from the screen. I found Waldo when you download the presentation, that's where he is.

18:21

So according to nist and their security control life cycle the first step in the process of a control label cycle is system categorization, which is based on a standard called fips 199, which is used to define the criticality and sensitivity of Information Systems, according to potential impact on business and tips 29 199 uses confidentiality integrity and availability.

18:49

I'll ability as the three categories and then they rank them by the impact low moderate and high impact on those potatoes that particular data sign confidentiality is who has access to Integrity who can modify availability is the business risk of loss of that system.

19:11

So as you go through and tag, obviously regulated data automatically, hi, it's confidential the Yeah, but in most cases we tag it as high we think it's easier just to look at it from that Viewpoint as you go through the rest of your information and want to go through this process and you look at each of your systems that you have on Sat on site and you'll tag them so high moderate low if you look at a system that's not regulated and say it's confidential as moderate and availability is moderate, but Integrity is high you always choose the high water mark when you label them system.

19:49

So in this case, we've labeled all of our systems and the second step is to create the proper boundaries around the information. So this is a PCI scoping exercise and what we've done with our clients.

20:03

And you said well, they're trying to protect cardholder data just as in manufacturing and departures you want to protect cui or in healthcare HIPAA an e Phi and so on and so on category 1 is regulated data or The crisis hi information is categorized as hot means it stores processes or transmits that type of information.

20:28

Category two systems are support systems or systems that require access into category 1 and in many cases You'll Think of domain controllers patch servers antivirus servers jump servers like RDS servers that need to access category 1 systems, then category three systems are everything outside of the boundary.

20:50

So they're not going to touch they're not going to be infectious from category 1 systems and they don't sort transfer process or even touch Related information. So as you take each of your systems you move them into the proper boundaries.

21:06

This allows you then to know where the data exists first you tag the data now, you've tagged your systems and the first step as I mentioned of a life cycle system categorization leads to choosing your controls documenting your controls implementing a controls authorizing systems to move into production and then monitor, you know managing an auditing your controls.

21:30

So once they've been moved in the proper boundary, you have Fitness logical boundary is now you can put in place some physical boundaries such as in a PCI environment restricted access into cardholder data environments is required using layers of and filtering explicit deny rules and access control lists that defined who has write access that information.

21:56

So this is how we reduce the scope of work. So we're moving the options what we see in the field is companies either apply all controls everything and there are some benefits it eliminates the need for system categorization or or data classification.

22:17

You don't have to go through that exercise because you're going to take your controls and flat all controls or you're going to call them a common control and apply them to all Such that it reduces the number of Transport data flow paths and storage platforms. Those are the Batman's on the challenge side. It doesn't consider not recycling station for Access Control or for lateral movement. One of the benefits of segmenting. Your not work properly is that if you get a piece of malware like Imhotep, which is very very fast and network aware and it infects a particular segment of that segment can see the other side.

22:56

Oh well that it can perform lateral movement and affect other systems part of these boundaries and separation lot of physical separation is to prevent that lateral movement. It adds complexity to access control configuration increases the number of systems require a logging. So if you're doing an audit logging and you're trying to audit for regulated information expands the attack surface and increases administrative overhead and cost me give you a quick example.

23:26

How that works. I worked with a automobile dealership at about 750 systems and they asked us to come in and perform a PCI assessment for them. Well when I got there only six systems in the credit department actually stored processor transmitted cardholder information yet the scope had to Encompass the entire 750 systems.

23:53

So all controls needed to be applied to All 750 systems. So the fix was simple. We put a firewall in between the credit department and the rest of the network with the proper rules applied and isolated the cardholder data environment. And now the PCI controls regulations and requirements are only applied to those success stems. So it clearly reduce the scope of the systems that fall under regulation and administrative around cost.

24:24

The other option is to follow the process that we talked about earlier and to apply your controls based on categorization level. So if you can isolate regulated data and put a boundary around it, then only the systems within that boundary are applicable.

24:42

We work in the energy cycle segment and in the energy sector of the power plants themselves fall under Nerf separate regulation, but the business offices do not So the goal is to isolate the power plants and not allow access from the business. I direct access or even internet access at the plant level to create better controls around that and then we only have to apply nourish that controls to the power plants and not to the business side of the energy cycle.

25:14

All right. Turn it back over to Ellen is going to get into more detail on the ACT. Thank you. Thank you. So, you know for the non-technical people probably some of what Michael said shot over, you know, certainly shot over my head and probably shot over a couple of other people's head as to all the ways to actually achieve it but the backstory to why we needed to do that is because this now the law the new section of the law the part coming out in March requires the organization to actually implement.

25:43

Controls and procedures and processes to do that. So what Michael was describing earlier were some of those controls processes and procedures we heard him in a lot of contexts like sip or so forth like that, but for the shield data the data protected by Shield you need to do the same thing. It's just that the path that the New York State Legislature is created in The Shield is actually a pretty well-trod track path in the sense that many organizations have done it in the context of HIPAA DFS.

26:13

Energy in the Merc Sip and so forth. But now we're seeing it for organizations that are subject to shield. And so all that stuff that makes talking about is is well known and done by many organizations and obviously IV for has a tremendous amount of experience helping people Implement those things, but now many organizations that didn't previously have to do it because they didn't have to comply with

those laws before now need to start thinking about good Lord. How am I going to do that in my company? And that's I think so.

26:43

Help to put in context. So who does he need to do the New York Shield stuff? Well, that's going to be basically any business no matter where they don't have to be in New York. They could be in California. They could be in Europe that could be anywhere that the u.s. Can get jurisdiction over right anywhere that holds personal data of the type. We described earlier in their systems, right and it applies to both regulated companies that we talked about the hip and Dirk sip DFS, which is Department of Financial Services.

27:13

Like insurance companies or Banks.

27:15

It applies to companies that are subject to gramm-leach-bliley act but it applies to them differently than it applies to the companies that haven't been regulated before and so it applies to everyone that holds New York State data and and it makes some allowances for companies that are smaller, but I'm not sure it's particularly helpful in the way it does that so let's talk about we'll get to that piece in a minute, but Let's talk about if you do experience a breach under the old under the first section than the part that went into effect October. What is it you need to do. So if there's a couple of ways you can have a breach right?

27:56

One of them is someone evil gets into your system and does all sorts of Mayhem mischief and exploring around that's I think the more traditional breach that people think about but you can also have a breach where someone is in your organization because to a file that they shouldn't have and they're there and you could even have someone that's authorized typically to get to this type of information, but they weren't supposed to get to that particular individuals information.

28:25

All of those now are reach under the new the new law if someone is authorized though, there's a little exception of someone is otherwise authorized to be in the database to see like a person but not the person that they happen to land on that could be inadvertent and if there's no harm To the person that they landed on then you don't have to give any one notification, but you do need to do an analysis to show that there was no harm you need to do a risk assessment from the point of view of the data subject of the individual whose record was landed upon and confirm that actually what happened while unfortunate while it's about something maybe we need to address with technical administrative or physical controls. So it doesn't happen again while it happened. It didn't actually pose a risk to the individual therefore.

29:13

We don't need to let anyone know you got to keep that analysis and if it involves a lot of people like 500 people are you got to keep that record for five years because the state in the law reserves the right to

go back and see if you were on the up-and-up when you made that analysis if they decided that you really found that reporting a breach of inconvenient embarrassing are expensive and on that basis, you decided not to report the breach that would in pretty badly. So it's important to keep the basis that you made that.

29:43

Nation so that if anyone comes back they can you can show that you document it and actually went through that analysis if though you decide there is a harm right The Intruders from the outside. It was not inadvertent to it was it was a bad thing. Then you have to do a couple of things. First thing you have to do is you have to let the State Attorney General the state policy. Sorry their state police and the Secretary of State know the event. So that's that's something you have to do and there's actually a form you can go to and fill that out.

30:13

Out although honestly, I would recommend you have a lawyer or someone do that on your behalf. Because it's It ultimately can be made public and you have to you know, you it's just it's better to have a little bit of a barrier between you and someone filing it for you.

30:28

There's also some art in crafting the words, but anyone can go there to the site and report a brief is not reserved it certainly no requirement that there be a lawyer just something to think about if you're in that situation if more than 5,000 residents of the state are You've got to let the correct their report to credit reporting companies know about it. So that is if they're not breached. But if you can you got to let them know so that so that they can take steps to protect the data subjects in the state. And you also need to let the affected residents know there's a whole mechanism that I won't go into because hopefully, you know, not many of you will have to go through it. But you have there's a whole mechanism in the form of the notice the manner of the notice how it goes.

31:11

What type of information You need to include in the notice, but you've got to let the data subjects know so they can take steps to protect themselves as a result of the breach. There are other regulations. Obviously that apply to notifying data subjects of the risks or HIPAA has that the gramm-leach-bliley DFS from these all have notification requirements as well. The state has decided that the shield law will be subordinate to those laws.

31:41

So if those laws have a report Mechanism, you must you'll report according to the requirements of those laws only if those laws don't have a reporting requirement, we default to the states reporting requirement. But even if you report under say HIPAA or DFS or some other you still need to report to the State Attorney General the state police and the secretary of state of the event. So you have to let the state know as well.

32:07

And you know, if the breeches big enough expect some follow-up inquiry and investigation that That's that's going to come. So, you know, once you have a breach in your letting people know it's super important to document it really well. Make sure the notices you're giving out our really well well written informative explanatory because if the breaches large enough for the information is sensitive enough. There's going to be some follow-up inquiry.

32:35

The state did create two categories of businesses Under The Shield law. The first one is a small business standard where if and it's not like you can pick the one of these that lets you get away with it. If anyone is these fails then then you're no longer a small business.

32:54

But if you have fewer than 50 million 50 employees if you have less than 3 million in growth revenue for the past three fiscal years or Less than 5 million a year in total assets and you can you know tick all those boxes then you can Define yourself as a small business under the law and the law gives a you know, I get it but it's a it's not a particularly helpful thing to understand what that means. Right? The law says reasonable administrative Technical and physical safeguards that are appropriate for the size and complexity of the small business and the nature and scope.

33:34

Of its activities and the sensitivities of the information it collects. So how you know how a small business that doesn't have a cyber security group an in-house legal team risk compliance group and so forth can decide now that these safeguards and and procedures and standards and policies. The Implement are reasonable under the situation of the data it collects I think is hard. It's actually in some ways making it harder for a small business.

34:04

Because the larger businesses have a more defined things that it must do this is sort of nebulous. So from you know, if the breach is bad enough, I guess it wasn't good enough, but if the reach wasn't so bad that what you did was good enough, which is kind of an unfair standard, but you know, I hopefully they're not going to do that, but we'll see. I don't know Mike if you have anything you want to know is not a fact the talked about this little bit about the small business space.

34:32

48% of all breaches are perpetrated against the SMB community and it's kind of putting a Target on their back by not giving them clearly defined controls that they can align to it makes it very difficult for them to understand what they need to implement especially like you said, we don't have a lot of technical expertise or security expertise on staff.

34:55

So I think there's real challenged organization and small business community and I'm going to make a suggestion on Talk about how much security as an obstacle ready? Yeah, I mean but it's hard right and it's time to start to think about that because March is coming Fast And for those small businesses, you know, they got to get a plan in place as to how they're going to do it and what what is reasonable under

the circumstances and definitely, you know, speak to your lawyer speak to technical consultants like Mike and and get some some comfort level as to what it is.

35:31

Is you know other standards like ffiec the defense department groups like that actually have defined things that you need to do depending upon the size of your organization the level of risk it here. The standard is pretty loose. So it's a little scary I think for a small business to figure out what it needs to do for the the larger businesses. And for those that want to read at home. It's under Section 8 99 section BB subsection 2 V which is the stuff that warms the heart.

36:01

Lawyers everywhere you can cite to a regulation, you know, they have 14 elements that I kind of convinced the 13 years. I didn't do that much of a favor that you need to do around the administrative Technical and physical safeguards. And so these are going to other companies that have more than 50 employees more than 5 million in assets are more than 2 million in Revenue over in any of the last three years.

36:27

So they're the first thing you do is worry about your administrative safeguards and my My please chime in if sure, you know, you want to put any technical color to these but you need to appoint someone who's going to be responsible for the security of your organization. You need to now have someone identified who is the individual responsible for who report to the board who will give management and oversight as to how security organization is.

36:51

So no longer can a board or a CEO or someone say, I didn't know they have to appoint someone who's actually going to do that role and keep them apprised and make sure that the organization Mission is actually implementing this policy. So anyone familiar with HIPAA or DFS currently, they both call out and hip US security officer and security responsibilities in DFS. The CSO attorneys be important in appointed internally or outsourced. So and I thought you know the GPR which is the European Privacy Law. They have a data Protection Officer.

37:25

So you're seeing all the modern laws that are coming out and help us out that modern frankly, but but you know a lot of the New laws are are requiring accountability and an individual level DFS require certification by the CEO or someone in chart of the organization that they're actually doing it. So there's a lot of individual accountability and we're seeing that here as well. You also need to identify all internal and external risks. That's what the law says, right? So, you know, how do you do that? That's that's hard. Right? So this is like a mission statement. Each of these are you know, for the corporate people, right?

37:59

These are the mission statements that Laws defining for you. You still need to have the tactics that Michael Campisi can go over a bit and how you know, his products helps for that. But you need to have a way that you can identify your internal and external risks. You've got to then assess the safeguards that

you have in place to guard against those risks. You've got to train people and manage your employees on best practices and how they're going to behave so as to reduce those risks you need to you.

38:31

Go find providers. You know, Mike just mentioned that you need qualified service providers and make sure that you have contractual obligations in place to ensure people are doing your vendors. All Mike at the beginning talk about all the data that's in the cloud. How do we make sure that those providers who are holding our data about New York residents are actually doing what they're supposed to do to protect that information. We need to adjust our program as our business changes or circumstances or the threat landscape changes.

39:00

We need to adjust Program continually that in the technical safeguards, you know, they want us to assess the risks in the network and software design. I mean that that's a mission statement. That doesn't tell you actually what you what you're going to do. It just tells you what you need to accomplish at the back end and getting there is actually pretty hard. So if this is not something your organization has faced before and you haven't really thought about it in a methodological way and documented that analysis that's this is a daunting task to do in the next couple of days.

39:31

You know March is coming fast. You can actually measure days you have to assess the risk in processing information transmission and storage. So, you know, that's that's a new thing. Right? What what is it? What what risk do the data subject phase? What risk does my organization face if I process the data stored or transmitted in some way we need to detect and respond to attacks and failures.

39:56

We need to test the effectiveness of key control systems and procedures and This is a funny one, right? Because you need to test the effectiveness of T control systems and procedures what I bet you a lot of the organizations out there in the state don't have heat controls and procedures that in and processes in place to protect the data they have they're doing and I you know, I have a ton of clients. I need a lot of them. I see it in the event. I see other lawyers that are in space all of our clients do security right they have security, but they don't document it.

40:29

They don't have controls in place that are actually making Making sure that that things are happening as they intended to happen at there's a systematic approach. So presuming that the law presumes that there are key controls in place. That's a big presumption you if you don't have you got to start creating them and that's time consuming. Then you got to have physical safeguards. So you need to assess what's the risk of how I'm storing information and I'm keeping it you need to detect and prevent to intrusion so that could be people coming into your office as well as how you're actually stopping people from logging on to your next.

41:01

Works and then the last thing here is you got to protect against unauthorised access to or the use of the private information for all processing activities. And these are literally elements in the law and they put section numbers next to each one of these things. So it's not like, you know, this is some it's-- dream right to the extent we have dreams. This is these are these are actually things that the legislature said you need to do. So, so they're they're bulleted out there.

41:32

And then the fines are bad, you know, if you think well good lord. I can't do any of this. I don't want to do this. This is more. I'll just hope it doesn't happen to me. They've increased the finds out or a quarter million or $20 per failed notice.

41:46

So, you know Mike at the beginning said that statistically he's seeing the cost of a breach at a hundred and thirty-four you said forty eight hundred and forty eight dollars a record, you know, in addition to that you can now get a 20 dollar fine per record up to The quarter million and a minimum of 5,000. So it's a you know, it's not a trivial thing. And then if you don't Implement these these controls the AG has the ability to enjoy new shut you down do a lot of other stuff the the one blessing in all of this is some states like Illinois for the biometric data has a law that allows for a private right of action.

42:23

So in that state like you're seeing class actions being brought where like people go to amusement park with a with a with a friend's mom or Something like that and one of the kids get scanned biometrically, they didn't get consent for the biometric scanning by the actual mother the amusement park doesn't know it just you know scans all the kids. Well that resulted in a pretty big class-action lawsuit, you know that, you know, they were using biometric to figure out if you're authorized to go on the ride or not. So it you know, that's so you don't have private right of action and that I think reduces it enables the sort of trolling or strike suits from prevents that from happening.

43:02

But it reaches bad enough, you know, it could be a problem.

43:07

Sorry, I went to look at the flight. So you know how much security is not so this is really going back to the talking about all of the requirements that the shield act has in place. It's what this is one of the common questions we get asked is and really our response is kind of awesome underwhelming. We usually say it depends lawyer answer you got a reason why is it's going to map out your security.

43:36

Requirements and with the procedures of how you implement those controls. There's a really wide variety in terms of how you enable you think of some of the other regulatory like HIPAA there are required components and their addressable components. So very wide berth in terms of how you get there in terms of especially in terms of The Shield act unlike things like mist and the 20 critical controls that are very very system center.

44:05

So there's specific about out what you need to do when Alan was speaking to each of those controls in the shield act the very broad which there were statements and their mission statements are high-level governance type statements as opposed to how you get there. So while there are 14 high-level requirements many of the standards based models like Miss 20 critical troll ISO 27000 are have hundreds of soft controls that help you define what the expectation is.

44:36

And you can find crosswalks too many of these control Frameworks. So if you're under HIPAA and you want to look at when a critical you fallen or PCI, you can look at the crosswalks between controls and I'm sure she'll will be added to that at some point. No help better to find that if previously you didn't have any regulatory requirement in this is new to you. You may want to go and it's a good starting point.

45:03

I think it's a great opportunity to evaluate the The current security program at align it with some basic standards. It probably would be beneficial to look at something especially if you're a smaller business like to see I asked 20 protocol controls that has a hundred and seventy two sub controls but are much more specific and better defined and then crosswalk those to the shield act requirements.

45:28

I think will help you get there much more expeditiously the other suggestion is if is too Crosswalk do a gap analysis. So take those controlled Frameworks and go through and perform a gap analysis for your own environment to determine what do we already have in place that aligns with requirements of the CEO of Apple and what are the Deltas where the gaps that we need to remediate build a poem and be able to then knock off the list to get to being compliant.

46:02

In the small business, you see I put a bunch of Statistics out there around the SMB space and you know while it's clearly defined for Enterprise you work with a lot of Enterprise organizations that align with Nestor 27,000 and it's easy to build those clams out but small businesses tend to have not adopted a control framework and you can see cyber attacks 43% We had one small business that we work with they were actually in architectural firm that Come bull ransomware. All their systems are encrypted including their backup. It took us about five weeks to get their backups to a state that we could recover them because of that. They were five days from going out of business. So size and scale is really not shouldn't be the Bellwether.

46:53

It's really about determining your organization's risk tolerance aligning your controls to mitigate your perception of risk and On top of that just keeping in mind that the threat landscape has changed a ransomware attacking hours every 14 seconds. They said by 2020 that's going to drop every 12 seconds. So it's really Securities be proportional but not at the expense of covers security hygiene.

47:20

And then I just want to go through a security spending model with you a lot of people trying to figure out what should I be budgeting for security Now statistically looking at the 2019 the average it budget came in around 2.7 percent of Revenue and that varies from a low of 2 percent to as high as 44.5% But the average is 2.7 percent of Revenue IBM recommends that the If the security budget should be 13.7 percent of that it budget. So it's really easy to just do the math. If you're a hundred million dollar business 2.7 million dollars allocated to it budget 370,000 should be allocated to security and so on I put the 3 million is the bottom because it relates back to Alan's point back at that. The different designations of The Shield act small business designation.

48:18

Was that three million dollars If you're spending $11,000 on security, it's probably not enough and you probably don't have the expertise and that's where it really comes into play. But this gives you some type of guideline to what budget should be in terms of it budget and security budget.

48:41

Now I'm going to turn it over to fight can be easy. You know, you're in the home stretch in the software guy gets a chance to talk. So again making PC with with seat, right? Thank you for participating. You know, it's in listening to Alan and Michael speak. It's it's really amazing to hear all the acronyms in the alphabet soup of regulations and Frameworks and try to understand what that means to your business. You know, bottom line is these regulations are asking organizations to do certain things to protect.

49:11

Data protect information protect the privacy of there's of residents and shields case. So organizations are required to do certain things. In this case. It's processes procedures and controls. We've been talking about them for the majority of this conversation. Now what's interesting about Shield is that it does specifically reference some other obligations that if you are previously regulated, you can leverage those as a part of your adherence to the law, but it does require you to take a look at those Information Systems to be re-evaluated to ensure the system.

49:41

Items not previously obligated to a regulation are now falling into that mix. So it's a critical piece of this conversation that you may you may already be HIPAA regulated or gramm-leach-bliley regulated with Shield. You can leverage those other controls that are in place, but you still have to take a look at the information systems that may not have been regulated by those acts that are now a part of that requirement. So it's an important thing to understand about this from from the processes and procedures perspective.

50:10

No, You can you can go through this process and Define these these controls in this thing's and translate regulations yourself if it made sense for your business, but the reality is that takes a ton of time and if you don't have the time or the resources or the Acumen to be able to do that, you need to rely on some other other areas to to get you to that end game. And in this case, you look in the screen here. We have the center for Internet Security.

50:38

We've got I so we've got now is we've got I saw Because Co bit you know, those are controls and processes and procedures that have already been written that are defined as industry standards that organizations can utilize to support their compliance obligations or the protection environment, whether they're regulated or not regulated. These are standards that can be used for best practice or to meet obligations at the regulatory level. And the other piece to all of this stuff is in Ellen referenced if you're not documenting what you're doing, you're not doing compliance because that's the first thing they're going to look for when an auditor comes in.

51:11

Is the documentation of the things you've got in place? So documenting is a critical part of that.

51:18

So the gratuitous would be webinar without some Shameless commercials to a captive audience. So how do how can software potentially help you get there and I'll specifically speak to sitra and the symmetric platform that we go to market with, you know, all these things you've heard and is it's usually done with limited resources limited funding particular at the smaller business level. How do you get there? It really comes down to as much automation.

51:48

You possibly can get in leveraging assets that they can help you get to that to the goal line within reason to your business. So he's logged down touched on earlier. These logs are really hard to translate into tactical initiatives.

52:02

If you try how do you know that what you're doing actually satisfies the requirements of the law and frankly, that's what we do at sitra with are symmetric platform is Leverage The Amazing mind power of lawyers like Alan to Translate these laws and actually map them to specific tactics that you can Implement to meet the obligations of the law. So as a part of what we do as an organization is, you know, once you understand what your obligations are going to be you go through the process of defining the risk and assessing it and then going through the process of assigning or the controls in the processes and procedures that are that are need to be put into place the information technology teams the security teams.

52:48

Don't need to translate regulations. They can actually take what is outputted from this particular platform and say listen, if I do these things not only am I meeting technical obligations, but I'm also meeting compliance obligations to the same time because all of its been vetted by the lawyers at Harris Beach. So it does take off a significant burden of upfront due diligence that can be done through an automation process that this symmetric brings to the table. The other part to that of course is then is to to Define and put into place.

53:18

Disease that your organization is marching towards and these are your goals here are to not only state that you have a policy but then be able to track and document the fact that you're doing all of these things and that's really what our platform is designed to do. And if you think about all of that as you as you evolve your program and you get to the point where you want to understand how far along you are in that process and how mature your program is.

53:43

The tool also walks you through that process to assess an audit your program and then Understand how you evolve it over time and where you can you go through that process. Where is your risk? Where is your risk most highly exposed and then address your resources to it to to adapt your program accordingly and evolve it as threats change as regulations change as your environment changes as you add new systems and new data elements to your plot to your organization. All those affect your policies and programs and normally you'd have to go back and regenerate your policies through a law firm or a lawyer.

54:18

Lawyer through the click of a button symmetrical I to do that automatically on the fly without so your your program can evolve and be dynamic and be current with with as much automation as possibly can be determined and I think at the end of the day, you know, all of this does require resources to help you get to that to that goal.

54:37

If you don't have the resources internally to help you with that organizations like Ivory for our purpose built to support that process and help you navigate this both from a from a People as well to operational perspective. And with that I'm going to turn this over back to Michael to close this thing out and kind of speak to what IV for does in the context of what we just went from this whole entire conversation. So, how can we help? We have a couple of Managed IT solutions programs that the first is we call GRC Mets Managed IT solution in its governance risk and compliance and really the reason that seeker and IV for here presenting together is that I looked at.

55:18

Their tool as I walk through this data discovery of classification. It's what we talked about earlier about where's my stuff? We have an automated process leveraging Azure information protection that we can data perform data classification and tagging. Once we know where your information is, we can help you with security control Gap analysis through series of workshops help you develop a poem a system security plan.

55:45

So system security plan is where the Who comes into play in our Inner Man of solution? We have partnered with sitra rather than using spreadsheets and Word Documents like many of you are probably using currently we wanted to automate the process. So we Leverage The symmetric platform for the development of your system security plan execution of the poem and then ongoing maintenance of that SSP along with change management or auditing on the technical side many of the controls that Ellen went through.

56:18

In the shield act we can help you satisfy. So in that cycle of assessing your controls remediating your controls are remediation. We have a team of security engineers and analysts that can deploy tools for vulnerability management security awareness training email hardening incident response plans, all of the technical components that are called out in the shield act. We have the ability to provide a managed service around many of those components.

56:51

Back down to close it out real quick. So the March March 23 is coming fast right hundred twenty-two days, 17 weeks for months, right? That's those are the big scary red dots there on the side and boy they come really fast. I mean just just trying to get around it. And by the way, there's a lot of you know Christmas Hanukkah Thanksgiving all these qualities holidays are in between so it's coming fast, right?

57:15

So first things you know bottom line is good to see so someone that Going to be shepherding this process through for your organization do that like right away and Empower them to do something so that they can they can fulfill their mission. Right? You've got to work with that fee. So to get a cyber security program in place build the controls and safeguards technical things that you're going to do to make it work. You've got to assess the program. You can probably do that after March, right, but you've got to get something in right?

57:45

It doesn't have to be perfect doesn't have to be a home run nice thing about symmetric and And that is that you don't have to get it right the first time it can be an evolving process but get something down and have it Justified. Even if it's not perfect right get something down so that come March your set then, you know get a training program in place of people understanding what they need to do. We start getting a grip around. Where is your data?

58:08

When it's not on one of your servers the cloud is, you know, as Michael said earlier the cloud is a huge amount of data is out there and you know, just because you don't it's not on Our system doesn't mean you're not responsible for it. It's still your data and you're still responsible to the New York State residents is to how your how how that organization that you've given it to is protecting it because they didn't choose to use it you're using it. So yuo, yuo the state residence a lot of protection around that information and you have to make sure they're doing it. Right. And the last thing is you have to be able to document the effectiveness of your program, you know with either a symmetric type tool or something else.

58:47

It could be the spreadsheet, but you've got to show Show that your program is actually doing what it what it's designed to do that that you got to get that all started by March 23, cuz cuz that's coming.

59:01

And I'm just going to start running through some of the questions. Thank you everyone who asked use the last three minutes or so to get those answered. If you do not get to your question. We will follow up with an email with the answer. So kicking it off with a couple questions about the small business standard number one do nonprofits count as a small business and number two, is it always fewer than 50 employees or can it just be based on dollar amount?

59:29

So the nonprofit's count right as long as you're holding the information of New York State residents, it counts and even counts of your the state. It's not the same law. It's not a Tenon on a a but even state agencies this law applies to under the 2 of section 208 of the technical law. So it does apply and you it's going to be if any one of those things fail then then you're going to be subject to the larger business one.

59:54

So, you know if you have 51 employees, but you only have two million I'd You're no longer in the small business one you're going to be coming into you're going to have to put the more formal process and document the more formal process of section 2 of 899 PD another question. How can you arrest a enforce this lot of businesses and other states that hold private information for New York State residents. Will they do it all the time and there's there's long-arm jurisdiction.

1:00:22

You can get you have there's jurisdiction across States California has a data Privacy Law that's pretty aggressive if If the New York State business takes and Miss handles, California data, they'll get it if a New York state business Miss handles European data, the Europeans will come across, you know, as long as as long as there's a jurisdictional arm that lets you reach across state lines, they'll get you and do public K through 12 educational institutions fall under this law. So if they're holding like drivers like I mean you go into a school now, my kids are in school I go in they scan my driver's license.

1:00:59

They're responsible to me when they scan my driver's license because they've got my name. They've got my picture. They've got my driver's license and ID there are there still there getting data.

1:01:10

It may not be student data may not be teacher or principal data, but it is data and I think pretty much every school is now scanning people's driver's licenses when they walk in so they are bringing themselves under the reporting requirements of shield and kind of in line with school does the add law to the requirements for Fulfill the shield act requirements. So it doesn't actually enumerate at law 2D in the regulatory scheme. Like it does with glba and HIPAA and the DFS section 508 of the of the regulation but I would argue, you know, no one's paying for this right so you can't sue me but I would argue that yes.

1:01:53

Yes, it does because if you look at law to D and its new regulation 121 That's a very defined things the school need to do and in my opinion anyway, for whatever that's worth. I think it's hyper aligned to the HIPAA requirements of the DFS requirements to the so when I look at that, I see that as a thoughtful

requirement for cyber security and therefore if you're doing those things you probably have the controls in place, but as Michael pointed out of very stupidly I think that you know, you met the ELA 2D protects teacher data principal.

1:02:29

And student data, but it doesn't protect the other types of data. So you if you're only applying the Ed law 2D to those systems that hold that type of data, you need to apply the shield type standards or the Ed law to d-type standards to the other systems that hold the data that pertains New York State residents. Sorry for the long answer on that one. Don't sign we're going to take maybe two more questions. And then if we didn't get to your question, we are going to follow up with a response from either Allen or Michael this afternoon.

1:02:59

But next one I think is probably a lot of people's minds is the C. So roll considered a true requirement of the shield Act.

1:03:08

Does it call out C. So it says it affect its dated that individuals need to be held accountable for security within the organization. I didn't see see so specifically called out there looking and just getting here so to felt being if it is data security, but it's following Implement administrative safe.

1:03:38

As designate one or more. It says designate one or more employees to secure coordinate the security program. So, you know coordinate the security program is to me a see so roll, but you know, you could call you could call the title the security program coordinator what they call it a security officer, right?

1:03:58

So it's I mean we use the we translate it to a see so because that's what most people think of it but to, you know, the person's role leaving aside the It'll is to coordinate the security program and be responsible for it. Yeah, it's responsibility is really the key who's going to be assigned responsibility over to the proper fish on the hook. What who done the hook. Yeah.

1:04:22

Okay, we've got a couple minutes over. So we're going to stop there again. We will be following up with your questions. Thank you. Everyone who submitted there were a lot of kind of Regulation specific questions. So we'll be sure to get back to you, you know, go to sitra dot IO for a demo of side metric and to learn more about their tool and visit IV for.com to learn more about our managed Services offerings. You will be getting an email with the recording of the webinar and an email with the slide deck.

1:04:51

Today and thanks so much for joining and that's it. Thank you everyone. Thank you.