PSC-ED-FSA-TISD

Moderator: Christal Simms
November 14, 2017
02:00 pm CT

Coordinator: Welcome and thank you for standing by. At this time all participants will be in a listen-only mode until the duration of today's conference.

This call is being recorded. If you have any objections you may disconnect at this time. May I introduce your speaker for today? Tiina Rodrigue. Please go ahead.

Tiina Rodrigue: Hello and welcome. I'm here to discuss postsecondary institution data security overview and requirements and to specifically into one of the tools (IHECF) that we have that'll assist you in making sure that you're compliant not only from a best practices perspective but also the regulatory requirements that you have as an institution, a state and federal basis.

Part of how we've built this agenda based off of the questions that we're asked when we're working with a school during the data breach so part of what we'd like to do is make sure that you have a general awareness of what the requirements are and then the specifics of how you can get to that exact checklist that you're looking for as you're working to improve your own security posture.

So part of what I'd like to start with is who needs to worry about data security. What I can tell you is that when I'm calling a school because they have a breach I start at the very top and I work with the President and the Board of Directors. They enter and pull in the CISO which is the Chief Information Security Officer, the Chief Information Officer (CIO). We work together typically with all of the registrars, comptrollers, treasurers, financial aid directors, Vice Presidents, faculty, and staff who may or may not have been directly involved with a breach and all the way down to the financial aid professionals, parents if they're involved as well as users, students, and applicants.

Conversely, I'll take a report from any and all of these people. While you may have a specific policy saying this person should report to the Department of Education, if I have any and all of these folks calling and say hey, I think there's been a problem - we'll begin an examination based off of even a single report on one record. It's important for you to know that everybody should be worried about data security from a greater perspective all the way up.

From an overarching perspective part of what we're trying to do is get schools to understand that when they're at this initial level of security which is where we find most of the education sector that we deal with and that they're at a very high risk, little maturity perspective. The information security activities are ad-hoc at best. There's no executive awareness. Sometimes the executive within the institution won't even want to take our calls and they think that purely it's a computer problem. They may or may not have a CISO. They may or may not have a formal program and users themselves aren't aware of their role. So the problem that we face is that the schools themselves are actually financial institutions.

They should be at least at a defined level of security maturity where they're proactive and they're taking this very seriously and they're working within a well-defined risk tolerance that's similar, working with goals in order to help them pull down their risk scores and make sure that they're more mature in as they build this formal information security program.

Part of the reason why it's so important is because educational institutions are being targeted for many reasons but it's in particular because their emails are worth money. What they're working with in terms of their research is worth money. Even the financial information is worth additional value as well. There are many reasons, many vectors why education is being attacked.

What we find is that we care about every single data breach because if a school has a breach, an initial breach may not be FSA data. If they don't respond to it appropriately, the bad guys will take a second bite at that apple and the next one will be (FSA data). We're working with schools that each and every indicator of a breach whether it's data, credentials, software, anything along that line because we know that ultimately our data is at risk because of an immature security posture within the school.

As I mentioned previously every school is a financial institution. This isn't just as assigned by Education. It also is per FTC and the Gramm-Leach-Bliley Act. Part of what we do is we enforce our Program Participation and Student Aid Internet Gateway Agreements and these further institute that having a secure school and being able to maintain a robust security program and posture falls under administrative capability.

Therefore if you don't have a robust posture then it could be that we'll have to yank your Title IV funds until you're administratively capable. This has already happened to multiple schools. The way that we look at a school is we examine their GLB safeguards and make sure that they're in place. These are relatively high level and they're of course determined by each school's risk profile.

Making sure that they develop an information security program that's documented; so they go through all of the steps that one would expect in an information security program - that there's someone who still works there who is in charge of that; that are some of the key elements that we look for as GLB safeguards, that they're making sure that the school is performing risk assessment on the three areas:

- training and management
- information systems but not just from a perimeter perspective, but also including software design, the storage processing, transmission, receiving, any part of the information life cycle to include disposal. (I can't tell you how many times I have run into situations where a school has improperly disposed of paper records and they have ended up having a breach recording against them) and then
- also making sure that if there's an ongoing attack intrusion, some sort of failure that a school can detect them or respond to them and thereby understand if they're well enough to prevent them.

When I began this webinar in person I often ask how many institutions in the room have already had a breach and typically very few hands are raised. That's when I share with them the fact that not having a raised hand is an indicator to me that they simply don't have the mechanisms in place, whether they be human systems, technological systems or administrative systems to detect the fact that they've had breaches or incidents of any kind.

Lastly we'll be looking to see how the risk assessments are resolved in controls to make sure that they are – that they take care of the risks that are identified and that, you know, if you don't have a direct control; that you have compensating control. For example, a padlock may be a compensating control in a situation where you can't have other ways to secure the data. And then those controls are regularly tested and monitored so saying that you're going to put something in a shack with a lock on it but not have any sort of testing or monitoring would be insufficient; say, if you had a million records sitting there. Someone could come up with bolt cutters, take off that padlock and get into the data.

You have to make sure that it's appropriate for the amount of risk that you're facing and that you're taking appropriate measures to detect, prevent and respond to any situation. Additionally, if you have a third-party service provider, say it's an IT provider or someone giving you a cloud service, anything along that line. You can never, never, never outsource the responsibility for the data.

You can outsource the service but it's still your duty to oversee the service provider to make sure that they are doing the appropriate steps and that they maintain the safeguard that you have – are responsible for and that you can control what they're doing and that you know in time if there's a breach. For example we had a school that told us that they just outsourced their security. And so something wasn't their responsibility anymore and again, that's not possible.

And then when they sent us a contract to prove what it was; the contracts were written in such a way that they didn't even reference GLBA. They didn't have the appropriate responsiveness with it and the school themselves had maintained the responsibility for security configuration, design, and test. Given that the issue had sprung into being in 2014 and we're talking about it in 2017; it was pretty clear that security design was negligent. Configuration wasn’t managed, either, since it involved a default password and testing was non-existent.

Suffice to say that if you decide to outsource and there’s a lot of great reasons why you’d want that; but you’re still in the driver’s seat when it comes to ensuring that you are fulfilling those safeguard responsibilities. Then last, but not least, as you have an information security program making sure that you evaluate and adjust what your program is as you have significant changes.

One of the things I like to suggest to an institution is that for example every time that they have a Presidential change or executive-leadership change, that’d be a great time to brush off the old information security program and update it, making sure that if you add colleges or if you change any of the underlying infrastructure or if you shrink any of those types of material changes - these are terrific times to modify your information security program documentation and the program itself. Those are all of the things that a school is required to do.

Additionally beyond (GLBA) there’s also a requirement to have an identity theft prevention program. That’s based off of the red flags rule. You’ll notice the rule requires a school can detect, prevent and respond to activities that indicate identity theft. That’s again a written program that will have to be developed and then delivered if you have a breach. I recommend that any and all schools that are participating in a Title IV program that they make sure that they have those written.

Now a breach per GLBA is section 314.4, Part B if not mistaken. They’re trying to prevent unauthorized disclosure, misuse, alteration, destruction or other compromise of information. It’s important to understand that unauthorized disclosure means showing data to someone who doesn’t have a need to know and specifically isn't authorized by the students or FSA to see that data.

Ultimately misuse is an authorized disclosure that's used for nefarious purposes, for example, we had one school where someone who was a financial aid professional was targeting women who had late submissions and promising them that he'd process the paperwork if they performed lewd acts. That'd constitute a misuse of data and would be considered a breach.

Altering data, destroying data is all defined by what the business purpose is and so specifically since it's – we're primarily carrying Title IV programs that'd be what we're discussing. However again we'll look at any breach to see whether or not the information security program that is supposed to be in place is actually as intended.

We're going to look at this not strictly from a technical perspective but administrative and physical perspective as well. In fact Bateau in 2011 showed that if an institution or organization relied strictly on technical safeguards that they'd actually be less secure than if they had the full set. We'll similarly be looking for that breadth as we do information security program reviews.

We're going to make sure that you're taking care of the security and confidentiality of the data, making sure that threats are protected against to ensure that the security and integrity is in place and that you have taken all appropriate measures to protect against unauthorized access disclosure, anything that'd cause harm or inconvenience to the customer.

One thing I really want to draw your attention to is the fact that while privacy laws in your state or area may have a minimum set of records, 300 records, 500 records, the GLB doesn't have a minimum size. Therefore if you have an unauthorized disclosure or something happened to even one record it's reportable. If it's an exposure to an employee that's also reportable; if it's someone who doesn't have a need-to-know.

If a student falls prey to a phishing attack and gives up their credentials for data that includes their financial records, that's reportable. It doesn't matter if it's a digital record, a paper record. It's reportable because data is data in whatever state it lives. We all want you to be aware that whether it's old data or new, whether it's paper data or digital data, whether the disclosure is by an employee to an employee or to an outsider it doesn't matter.

If it's not an authorized individual with a need-to-know it counts as a breach. Paper counts as a breach and it doesn't matter of it's in storage, in transit or being processed. Similarly it doesn't matter if it happens because of a technical glitch in your software or not. If there's an unauthorized disclosure, if there's a possibility or configuration that could cause that it's a breach and it should be disclosed.

This question comes up a lot of how or when do I report a breach. Specifically it's on the day you detected it. Your institution shouldn't do a full investigation to confirm or deny at the moment that you suspect that you have a breach. You should report it. It's described in the SAIG as immediately which typically means within the hour but on the day without question. On the day that you detect or suspect a breach is when it should be reported to Department of Education.

We have the authority to fine institutions, to remove Title IV aid and we could take all sorts of action under 34 CFR subpart G. Please be well aware of that if you're unable or unwilling…if you're unable to report that'd be one thing.

But if you're unwilling and we see a pattern and practice of not self-reporting breaches then we could in fact cause fines and further action.

This shouldn't be new news. There have been several to your colleagues letters, GEN-15-18, GEN-16-12 and others along with electronic announcements via annual FSA handbook plus the agreements themselves for program participation and the SAIG. To report a breach is relatively straightforward. Send an email. I'd prefer that you include this data to include the data breach impact method, who's your point of contact, email and telephone, remediation status and next steps.

That should all be in the email to cpssaig@ed.gov. However if your systems are hacked to the point where you can't send an email; we'll take a phone call. You can certainly call the education security operation center, EDSOC at 202-245-6550 and it operates 7 by 24. They'll take your call. Please note Tiina Rodrigue doesn't sit there. You can't get me through that number. If for some reason you want it directly to me you certainly can. My email again tiina.rodrigue@ed.gov and my direct line is 202-377-3887. You can get a hold of me any which way.

And so one of the things we've also done because we've run into so many schools that don't know their risk and don't understand what they are in a security maturity continuum. We have an automated cyber security assessment tool. It was originally built by the FFIEC but now we have made it simpler by automating the form itself and by adding a score card at the end so that it matches where you are versus where you should be and you can see your exact gaps.

This is an optional self-assessment tool that allows you to see exactly where you are in terms of that continuum and see what else you need to do from a best practices perspective, keeping in mind that you're a financial institution. As you're using the tool you may determine that you have certain aspects that don't apply. Just put those in the least category but trust and believe that as we look at the entire perspective of schools that we cover from the smallest mom-and-pop school all the way up to the grandest educational facility that you can imagine that any number, if not all of these are covered within the higher education realm.

Just as important is making sure that you're compliant. One of the things that education has done is set up a public/private partnership to reduce the burden of compliance for security and privacy controls. Part of how we've done that is we've created a framework that allows you to go in with a free account and lets you see how your state law is and compare it to GLB and create a checklist for consolidated controls.

For foreign schools there are actually international regulations. At the free account level, you get GLB, Red Flags and your state privacy laws. If you wanted to add HEA, FERPA, some of the other publications or rules that make that you'd have to get at the premium level but for free you can definitely get GLBA, Red Flags and your state regulations.

What that does is it de-duplicates the compliance controls and so then you know more than from just a best practices perspective but from a regulatory perspective what you need to have in place. It will prevent duplicate effort. It consolidates into that simple checklist so that even a non-IT professional can understand precisely what they need to do. It saves you time, money and effort of which nobody has enough.

In order to use this tool it's relatively straightforward. You'd go to (ed.commoncontrolshub.com) and you'll see a simple login screen. Now if you don't already have an account this is your opportunity to create an account on the upper right hand side. You just register with your email address and password and they'll get you set up relatively quickly.

Once you log in it's a relatively straight shot. You can create a list that has each state privacy laws, 16 CFR part 314-C, on the GLB safeguard rules add mentioned previously and then the red flags rule. So all of the things that we've covered today as requirements plus your state privacy laws will be available for you to select and then de-conflicted.

What that creates for you is this checklist of mandated and implied controls, mandated where it says it explicitly, implied means that in order to be compliant you'd have to have this control in place. It shows you the interrelationship between the law, what happens when you have multiple laws in place and then ensuring that you know the specific requirements for each control.

Let's say that you're creating a situation where you have multiple privacy laws in your state plus multiple federal regulations. You'd know exactly what's required and to what degree by each and every one of those. This is an example in the screen shot of what the controls are. As you see it you'll see that GLB is there, red flags rule as well as…this one is a Massachusetts example. You can see precisely what – on the leadership audits monitoring, human resources, operational management, all of the different levels of controls that are necessary.

You can keep clicking and drilling down so that you can understand precisely what you have and what you need to have. That way you can use the CAT tool as your inventory of what you already have in place and you see the regulations against this control list and find further what your regulatory gaps are, not just your best practice gaps. Even better this will allow you to have the detailed guidance so that you have your privacy protection in place for information and data. You can make sure that you have a personal data definition for every single aspect and that you can create those notifications as needed depending on who is the regulatory supervisor for any of the logs.

For example Department of Education requires that you notify us based off GLBA. We're not the regulatory authority for that. We just have a contractual agreement based off Title IV. What we have is Title IV regulatory authority and so we're monitoring who is administratively capable based off of many aspects to include fiduciary duty but administrative capability is one of which includes maintaining a strong cybersecurity stance.

All of that is included here so you have detailed guidance. If you're confused in any way the (IHECF) can help you. Then you can also – let's say you're a multi-region school - You can compare to other states to see whether or not something changes depending on what the situation is, what the laws are. So you can do specific comparison or you can consolidate them and include multiple states' laws so that let's say you know that since you have multi-region school you have to be compliant with all of that. Your data is set up in a consolidated way and it doesn't matter if it's Texas data or California data or Massachusetts data. You have to protect it; so that way you can do the comparison to make sure that you're compliant given all the controls. You don't have to worry about whether or not you're only fit for one of your locations, that you can cover all of them. And then additionally one of the things that this framework allows you to do is get access especially with the premium subscription, access to the most current laws, additional regulation standards, best practices. This may be of special importance if you're an international school.

You can add in your own documents based off of laws so that you have that aspect. If there's something that you don't see you can create it yourself and create more lists. You can help build that, export it so that you can give it to other people who aren't in the tool and then you can track your progress in the attestation portal itself. Then, depending on your situation you may even need custom spreadsheets so that you can do asset tracking, auditing, anything from multiple responsibilities down to providing compliance evidence if you're at an investigatory or examination situation.

That's part of it. The attestation portal as shown here gets to the point where you can create that evidence that you may need in your situation. This is again based off a Massachusetts example showing how you can prove that you have this compliance aspect in place and that you have been very mindful and thoughtful in your compliance audit.

That is part of what you can do from both of a free and a premium situation. Last but not least you can in the portal add and other missed guidelines, for example 800-171. It is something we recommend for our schools per GEN-16-12 and it covers all of these areas.

Let's say you want to get to that best practice or if you wanted to add FFIEC. You could add all of these into the compliance framework and see how they overlap, what you need to add, how you can get to that optimal security posture where your risks are minimized and your maturity is exactly where you need it to be to manage your risk tolerance. That's something you can do.

You could just do this manually, independently as well but frankly speaking of someone who has done that independently you wouldn't prefer to do it. You'd much rather have a tool like this that saves you weeks of time and effort, if only into looking up in the analysis that only the actually putting in place your security.

That is where we're at. If anybody sees this webinar and has any questions you can email them to tiina.rodrigue@ed.gov. That's T-I-I-N-A dot Rodrigue, R-O-D-R-I-G-U-E at ED dot GOV. I'll look forward to receiving them and answering them. I'll publish them if appropriate on the IFAP.ed.gov site that's available. Just look for Cybersecurity Compliance on the right hand side of the page and that'll allow you to have everything you need to review any and all of what we've shared today. It gets you direct access to this tool as well.

Thank you very much for your time and if you have any questions, again tiina.rodrigue@ed.gov.

END