Question and Answers from the Cybersecurity Tips and Tools – "SB820 and Hb3834 (86th) Impact and Requirements to Texas school districts"

September 11, 2019

Q: What is the difference between TAC 202 and the Texas Cybersecurity Framework? Is TAC 202 a component of the TCF, or are they separate documents?

They are separate statutes. TAC 202 is the Texas Administrative Code for agencies and institutes of higher education. The Texas Cybersecurity Framework was adopted by the Department of Information Resources under Chapters 2054 and 2059, Government Code as the information security standards for institutions of higher education and state agencies.

Q: Where did he get the spread sheet that have the roadmap?

The Texas Cybersecurity Framework self-assessment spreadsheet can be found at https://www.texasgateway.org/resource/cybersecurity-tips-and-tools under Texas Cybersecurity Framework.

Q: Where may I get a copy of this presentation?

The presentation slides and video of the presentation have been uploaded to the Texas gateway portal at https://www.texasgateway.org/resource/cybersecurity-tips-and-tools.

Q: Do you know anything about the cybersecurity policy TASB is writing for districts to adopt in response to SB 820?

TASB provides districts with policies more focused on school districts operations, but they typically do not include information regarding cybersecurity.

Q: Where is, the Self-Assessment located for Cybersecurity Objectives?

The Texas Cybersecurity Framework self-assessment spreadsheet can be found at https://www.texasgateway.org/resource/cybersecurity-tips-and-tools under Texas Cybersecurity Framework.

Q: Where is the URL for the Redbook?

The latest version of the Incident Response Team Redbook is dated April 2019 and can be found at https://www.texasgateway.org/sites/default/files/resources/documents/TEA%20Incident%20Response%20Template_September%202017.pdf at the bottom of the website Related Items/Documents

Q: Will TEA require ISDs to adhere to the Texas Cybersecurity Framework to comply with SB.820, or can ISDs choose to follow other frameworks? Has TEA identified other frameworks that can be used to comply with SB.820?

ISD's may chose other frameworks which will protect the districts cyberinfrastructure, determine risks and implement mitigation planning (as required in SB820) if the cybersecurity policy does not conflict with Texas Cybersecurity Framework (TCF) as stated in SB820. TEA and the regional support centers are required by Texas Government Code to use the TCF and can aid and guidance on its use. The TCF is based and mapped to the National Institute for Standards and Technology (NIST) Cybersecurity Framework. Other frameworks that might be considered are the NIST Cybersecurity Framework https://www.nist.gov/cybersecurityframework and the CIS RAM (Center for Internet Security® Risk Assessment Method) https://learn.cisecurity.org/cis-ram.

Q: Is there any way to mask our email address to prevent them from being crawled online on TEA's website or AskTED and added to mass emailers?

There currently is not a statute protecting this type of information from Public Information Requests.

Q: Do we report every single cybersecurity incident? (i.e. hardware failure) or just the loss of student/staff information?

SB820 only requires districts to report a breach of system security involving student PII information. TEA has established a special email address to receive this type of information. cybersecurity@tea.texas.gov. Your ESC is also a resource when you have detected a cybersecurity event. Please feel free to reach out to the ESC's or TEA should you have questions or need assistance with any cybersecurity matter.

Q: Does the cybersecurity coordinator have to be a district employee or can it be a consultant hired for the role?

SB820 does not specify the cybersecurity coordinator must be an employee.

Is HB 3834 an unfunded mandate?

There was no additional funding allocated in HB3834.

Q: Do you know why the 25% rule only applies to state agencies? We have hundreds of employees who may only use a district computer or email account 1-2 times a year and who may not speak English.

HB3834 requires local governments to identify employees with access to a local government computer system to take the required security awareness training. Phishing emails is a major avenue used to distribute malicious code including ransomware. It only takes one click to potentially create a major cybersecurity attack and disrupt or shutdown the cybersecurity infrastructure. I recommend anyone with access to the school district email take the training. DIR is researching the ability to

provide the training in multiple languages.

Q: Is there any funding provided to purchase the DIR approved cybersecurity training programs?

There was no additional funding allocated in HB3834.

Q: how does the state define a local computer system or database? Is it any computer system or only if they are considered critical or store/access confidential data?

HB3834 requires local governments to identify employees with access to a local government computer system to take the required security awareness training. Phishing emails is a major avenue used to distribute malicious code including ransomware. It only takes one click to potentially create a major cybersecurity attack and disrupt or shutdown the cybersecurity infrastructure. I recommend anyone with access to the school district email take the training.

Q: Do we have the updated sample template that guides through writing the policy that secures the district infrastructure, risk and mitigation plan at texasgateway.org?

The Texas Cybersecurity Framework self-assessment spreadsheet can be found at https://www.texasgateway.org/resource/cybersecurity-tips-and-tools under Texas Cybersecurity Framework.

Q: Our District just completed a district-wide risk assessment based on CIS Controls, will this be ok under new rules?

The CIS RAM (Center for Internet Security® Risk Assessment Method) is based on the NIST Cybersecurity Framework and can be located at https://learn.cisecurity.org/cis-ram. The CIS-RAM should not conflict with the Texas Cybersecurity Framework.

Q: Is there a listing of sensitive, protected, and confidential student information?

We have added a document called Sensitive Information Guidelines-TEA to the https://www.texasgateway.org/resource/cybersecurity-tips-and-tools

Q: Are temp employees/teacher, food service staff, and bus drivers required to do training?

HB3834 requires local governments to identify employees with access to a local government computer system to take the required security awareness training. Phishing emails is a major avenue used to distribute malicious code including ransomware. It only takes one click to potentially create a major cybersecurity attack and disrupt or shutdown the cybersecurity infrastructure. I recommend anyone with access to the school district email take the training.

Q: Are there any financial consequences if we aren't complaint with SB820?

SB820 does not provide any financial consequences for non-compliance.

Q: Who is responsible for performing the periodic audits with HB3834? [

HB3834 states: The governing body shall:
(2) require periodic audits to ensure compliance with this section. My interpretation would be the local government or school district.

Q: A school district's cybersecurity policy may not conflict with the information security standards for institutions of higher education. Does this not refer to TAC 202?

SB820 states: c) School district's cybersecurity policy may not conflict with the information security standards for institutions of higher education adopted by the Department of Information Resources under Chapters 2054 and 2059, Government Code. (Texas Cybersecurity Framework) not Texas Administrative Code 202.

Q: Will there be funding and grants given to assist with the Texas Cybersecurity Framework?

There was no additional funding allocated in SB820. I am not aware of any grants to assist with cybersecurity issues.

Q: Our District just purchased a phishing test management application as well as a library of cybersecurity-related training videos from the same vendor, who do we need to contact to ask for the vendor to be considered under HB 3834?

I would recommend contacting the vendor and see if they have applied for certification via DIR as required in HB3834.

Q: Do school districts have to complete the HEISC Tool that is on TX Gateway under Cybersecurity Tips & Tools. It's 101 items.

No. It is just a resource that can be used by school districts.

Q: Will there be a yearly audit of the 40 controls?

There is no require in SB820 for audits or reviews of the Texas Cybersecurity Framework or any other framework chosen by districts.

Q: Can we use CIS 20 as our framework in order to meet SB820 or do we HAVE to use Texas CSF? CIS20 also has a useful portal to track your continued cybersecurity growth.

The CIS RAM (Center for Internet Security® Risk Assessment Method) should not conflict with the Texas Cybersecurity Framework. More information can be found at https://learn.cisecurity.org/cis-ram.CIS RAM (Center for Internet Security® Risk Assessment Method) https://learn.cisecurity.org/cis-ram.

Q: I would like to get signed up for DSAC?

Just send me an email at frosty.walker@tea.texas.gov requesting to join and I can add you to the distribution list.

Q: For the reporting requirements, are we to report attempts that students/internal users make to circumvent filters or injecting a virus/malware from a BYOD connected to the network?

SB820 only required school districts to report cybersecurity issues involving a data breach of sensitive student data.

Q: Where can we download the framework and road map?

The Texas Cybersecurity Framework self-assessment spreadsheet can be found at https://www.texasgateway.org/resource/cybersecurity-tips-and-tools under Texas Cybersecurity Framework.

Q: Is there a timeframe for identifying the cybersecurity coordinator?

There has not been a timeframe established by TEA. We would like to have all the information input into AskTed by the Holidays.

Q: Redbook?

The latest version of the Incident Response Team Redbook is dated April 2019 and can be found at https://www.texasgateway.org/sites/default/files/resources/documents/TEA%20Incident%20Response%20Template_September%202017.pdf at the bottom of the website Related Items/Documents

Q: What's the timeline due date to have this in place for all Texas LEAs. It mentions 09/2019

Using a framework to protect the cybersecurity infrastructure, identify risk and develop migration planning takes time. I would expect the districts to have all three components by the start of FY2021-2022.

Q: Do you know anything about the Cyber INfo Sharing Org being established by SB64 for information exchanges?

I am aware that SB64 requires DIR to establish an information sharing and analysis organization. DIR hope to have the initial operational planning completed by early 2020.

Q: if we learn about a data security incident with a vendor that included our data, that happened before sept1st, but we're just learning about now, does that now need to be reported. we are

not in the that situation, but did just learn of an incident that happened last Nov. and we just found out a couple months ago?

I recommend reporting the issue. The more information we can collect the more we can provide to the legislation such as the cost of total time involved and the potential overall cost to resolve the issue.

Q: all superintendent email addresses are available in AskTed?

Yes, superintendent email address is available in AskTed.

Q: Is there a sample cybersecurity policy that districts can use to develop its own policy?

The Texas Cybersecurity Framework self-assessment spreadsheet can be found at https://www.texasgateway.org/resource/cybersecurity-tips-and-tools under Texas Cybersecurity Framework.

Q: Are there any "Cyber Security Policy" templates available that meet the requirements of the SB?

The Texas Cybersecurity Framework self-assessment spreadsheet can be found at https://www.texasgateway.org/resource/cybersecurity-tips-and-tools under Texas Cybersecurity Framework.

Q: Is it OK to publish school email addresses on our web page? Or should we NOT publish them?

Section 552.137 of the Texas Government Code states a personal email address is confidential (this does not include the work email address of a government employee).

Q: Regarding email addresses question, the email addresses are listed to the public on AskTed and available in a downloadable file. We've suspected that's where some spammers get email addresses

http://mansfield.tea.state.tx.us/TEA.AskTED.Web/Forms/ViewDirectory.aspx

Q: Are reports of cybersecurity incidents we make to TEA subject to open records requests?

Per Texas Government Code 552.139 Section (b)(4)

(b) The following information is confidential:

(4) information directly arising from a governmental body's routine efforts to prevent, detect, investigate, or mitigate a computer security incident, including information contained in or derived from an information security log.

(b-1) Subsection (b)(4) does not affect the notification requirements related to a breach of system security as defined by Section 521.053, Business & Commerce Code.

Q: Can an ESC function as THE coordinator for several school districts that might lack resources

There are no requirements in SB820 that the cybersecurity coordinator to be an employee of the district.

Q: Can we, a school district, use the IT security policies template found on Texas Gateway? and will this template cover the 40 subjects on the cybersecurity framework.

Yes, school districts may use the IT security polices template found on the Texas Gateway. The Texas Cybersecurity Framework self-assessment spreadsheet can be found at https://www.texasgateway.org/resource/cybersecurity-tips-and-tools under Texas Cybersecurity Framework.

Q: If you appoint an employee of the district how much would be a reasonable amount to pay that employee? Not sure what the coordinator position value.

Per LinkedIn a cybersecurity coordinator average salary range is $39.6K-$74.6K.

Q: How / where will we find out about approved DIR training programs? You mentioned that approved programs are expected in October, correct? Where will we find that list?

https://dir.texas.gov/View-About-DIR/Information-Security/Pages/Content.aspx?id=154

Q: Do policy templates exist for the policy mentioned in the 40 controls?

The Texas Cybersecurity Framework self-assessment spreadsheet can be found at https://www.texasgateway.org/resource/cybersecurity-tips-and-tools under Texas Cybersecurity Framework.

Q: Does the framework address cloud services beyond access controls? Has there been any discussion of 3rd party risk assessment?

The Texas Cybersecurity Framework address cloud services. The webinar entitled "Cybersecurity Tips and Tools - Simplifying the Texas Cybersecurity Framework" discusses some of the cloud services issues. I would recommend a 3rd party risk assessment every couple of years just to make sure your self-assessment is on track.

Q: I thought the cybersecurity training was for all employees that use the computer for their job 25% of the time and not all employees.

HB3834 requires state agencies to identify all employees which use computer systems

more than 25% and provide them with certified training. Local governments (including school districts) are required to provide certified security awareness training to all employees with access to computer systems. TEA requires all employees, contractors, interns including anyone receives an UserID to take security awareness training. Even our visiting auditors are required to take the training if the request an UserID.

Q: Great session. Thank you as always, Frosty!

Q: What about vendors that have student data on their servers (cloud based systems) How do we address their policies/security.

Vendor policies and security should be addressed in your contract Term and Conditions.

Q: Can you provide a list of school districts that have been attacked by ransomware and the approximate costs associated with their recovery?

All the school districts that have reported ransomware acts are working with the FBI and are still open law enforcement cases. This information is considered confidential under Texas Government Code 552.139 Section b (4).