Questions and Answers for the January 29th, 2020 GoToWebinar - Cybersecurity Tips and Tools – SB 820 and HB 3834 (86th) Updates for Texas school districts

Q: how does a district report a breach? is there a portal or official form?

A district report a breach by emailing TEA at cybersecurity@tea.texas.gov. An incident reporting template has been distributed to all designated Cybersecurity Coordinators will valid email addresses in AskTED.

Q: Regarding student information breaches, does that entail things such as email accounts getting compromised or accounts on other school resources getting compromised?

If the school district has declared FERPA directory information such as student's name, email address, photo, grade level, any of the directory information would not be considered as sensitive information unless parents have opted out of sharing that type of information, which would then qualify the directory information as sensitive. A typical list of sensitive or PII information as defined by FERPA or state statue is provided as resource on https://www.texasgateway.org/resource/cybersecurity-tips-and-tools at the bottom of the page.

Q: Will 800-53 be the controls from NIST we want to consider?

Yes, NIST 800-053 controls along with the NIST Framework would not conflict with the Texas Cybersecurity Framework as required in SB 820. The Texas Cybersecurity Framework is based on the NIST 800-053 controls as well.

Q: How does the cybersecurity plan apply to G-Suite environment? Student on times require apps from 3rd parties to complete assignments. Usually 3rd party advise the will capture student info like their names, etc.

If the school district has a contract with the 3rd party or the 3rd party is acting as an agent of the district, then the 3rd party is also responsible for FERPA compliance. Therefore, information identified as accessible by the 3rd party by the school district would not be unauthorized exposure.

Q: does a school board fall under the requirements of HB 3834?

Yes, elected officials are required to complete cybersecurity training regardless of whether they have access to a local government computer system or database. If the school board members are elected, then they are required to take the training.

Q: Will each employee reports their training, or can the district upload the list of employees that have been trained?

Per DIR's current website: "Local government employees (which school districts) will self-report their training compliance using Texas by Texas (TxT). The

expected launch date for this application is February 2020. In June, DIR will send a detailed report from the TxT application to each local government entity to verify training compliance. Although the self-reporting capability will not be available until early February, employees can take their certified cybersecurity training at any time prior to June 14, 2020."

Q: So each individual employee will have to report their training and we won't know if they did it or not until after the due date?

The school district should be keeping a record of who has completed the required training and at any time can verify who has or who has not completed the program.

Q: I was told by TX DIR that we would not have to use this new system to self report since schools are not prepared. Can we report as a district?

Per DIR's current website: "Local government employees (which school districts) will self-report their training compliance using Texas by Texas (TxT). The expected launch date for this application is February 2020. In June, DIR will send a detailed report from the TxT application to each local government entity to verify training compliance. Although the self-reporting capability will not be available until early February, employees can take their certified cybersecurity training at any time prior to June 14, 2020."

Q: So staff will have to report their training individually to the state? Not as a district? Also what are the implications of not completing the training by the due date for individual employees/district as a whole?

The school district should be keeping a record of who has completed the required training and at any time can verify who has or who has not completed the program. It is the responsibility of the school district to verify all employees have taken the required training.

Q: do those training need to be certified by the state?

No, just the program must be certified unless the school district has filed a Local Government Cybersecurity Training a& Awareness Program Exception Form which does have specific requirements. More information is available on the form which can be found at https://www.surveygizmo.com/s3/5182254/Local-Government-Cybersecurity-Training-Awareness-Program-Exception-Form

Q: Will you send us the slide show so that we can access the links?

The webinar slides and presentation along with the Questions and Answers for the session will be posted at: https://www.texasgateway.org/resource/cybersecurity-tips-and-tools.

Q: Also, given a specific program is approved, there are a list of courses under that program. Are they to all be completed for a given provider?

Each certified program may contain several modules/chapters of content which

are required to be completed prior to a record of completion is issued.

Q: Where is the website with the list of certified programs?

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

Q: Have any certifications been identified for organization CSO's?

None have been required for now; however, below is a list of that those interested in getting certified should consider:

CEH (Certified Ethical Hacker)
OSCP (Offensive Security Certified Professional)
CISA (Certified Information Security Auditor)
GCIH (GIAC Certified Incident Handler)
Certified Information Systems Security Professional (CISSP)

Q: Can an assessment be used to qualify an employee as completing training assuming the employee passes the assessment?

HB 3834 required all employees with access to a local government computer or database is required to complete a certified Security Awareness Training annually.

Q: Can we get our own cybersecurity awareness program certified by DIR and if so, what is the process particularly how long it takes to process?

Yes, A local government that employs a 'dedicated information resources cybersecurity officer' may use a cybersecurity training program that satisfies the statutory content requirements. In this scenario, training program certification is not required. The Local Government Cybersecurity Training a& Awareness Program Exception Form can be found at:
https://www.surveygizmo.com/s3/5182254/Local-Government-Cybersecurity-Training-Awareness-Program-Exception-Form

Q: Will each employee need to create their own ID in the TxT portal in order to self-report completion of the training? We may have over 4,000 employees needing to complete the training.

Yes, each employee can create the own ID in the TxT portal.

Q: What is the timeline for the notifying parents from the time of the incident.

Below is Section 521.053 of the Texas Business Code regarding Notification of a breach of system security:

Sec. 521.053. NOTIFICATION REQUIRED FOLLOWING BREACH OF SECURITY OF COMPUTERIZED DATA. (a) In this section, "breach of system security" means unauthorized acquisition of computerized

data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data. Good faith acquisition of sensitive personal information by an employee or agent of the person for the purposes of the person is not a breach of system security unless the person uses or discloses the sensitive personal information in an unauthorized manner.

(b) A person who conducts business in this state and owns or licenses computerized data that includes sensitive personal information shall disclose any breach of system security, after discovering or receiving notification of the breach, to any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made without unreasonable delay and in each case not later than the 60th day after the date on which the person determines that the breach occurred, except as provided by Subsection (d) or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

d) A person may delay providing notice as required by Subsection (b) or (c) at the request of a law enforcement agency that determines that the notification will impede a criminal investigation. The notification shall be made as soon as the law enforcement agency determines that the notification will not compromise the investigation.

Q: Is there a possibility that Districts will be able to mass report their 3834 data instead of requiring thousands of staff to self-report?

Per DIR's current website: "Local government employees (which school districts) will self-report their training compliance using Texas by Texas (TxT). The expected launch date for this application is February 2020. In June, DIR will send a detailed report from the TxT application to each local government entity to verify training compliance. Although the self-reporting capability will not be available until early February, employees can take their certified cybersecurity training at any time prior to June 14, 2020."

Q: If a student's account is used for something outside of the school district/cirricululm, such as a game

site, and that site gets compromised with that student account, would that be something that would need to be reported if/when we discover that?

If the website does not belong to a 3rd party acting as an agent for the school (i.e. gaming website personal email website), in this case the school would not be obligated to report it as a data breach exposure.

Q: Would it possible a standardized template when reporting a breach?

Yes, a standardized template is being developed and with be distribute to as Cybersecurity Coordinators.

Q: Would a compromised login with no loss of information need to be reported?

No, if in reviewing the application(s) logs and it is determined the login was not used after the compromise it would not need to be reported.

Q: Most vendors provide electronic reports for training completion. Can a district submit this on the behalf of employees instead of each employee having to self-report?

Per DIR's current website: "Local government employees (which school districts) will self-report their training compliance using Texas by Texas (TxT). The expected launch date for this application is February 2020. In June, DIR will send a detailed report from the TxT application to each local government entity to verify training compliance. Although the self-reporting capability will not be available until early February, employees can take their certified cybersecurity training at any time prior to June 14, 2020."

Q: What are the consequences to personnel or school if some people do not complete the cybersecurity training? I know the goal is 100%, but is there an acceptable percentage of personnel not completing the training?

HB 3834 requires employees and elected officials of the local government to complete a certified cybersecurity training program annually and the governing body shall verify the completion.

Q: Does the personnel need to complete the 5 required training courses by June 2020?

Yes, the school district will need to select the most appropriate certified training from the DIR list for the employees to complete. Employees will need to complete the training by June 143, 2020 when the verification process will start.

Q: To be clear regarding the reporting of training, it would rely on the employees to self report that they themselves have completed the training rather than the district as a whole reporting that they have completed it?

Per DIR's current website: "Local government employees (which school districts) will self-report their training compliance using Texas by Texas (TxT). The expected launch date for this application is February 2020. In June, DIR will send a detailed report from the TxT application to each local government entity to verify training compliance. Although the self-reporting capability will not be

available until early February, employees can take their certified cybersecurity training at any time prior to June 14, 2020." The verification process will start after June 14, 2020.

Q: This may have been covered before, and is already available, but is there a resources that shows current attack trends? ex. Tactics, Techniques and Procedures, number of incidents?

The Multi-State Information Sharing & Analysis Center (MS-ISAC) is a great resource for Cybersecurity Threats and information.
https://www.cisecurity.org/ms-isac/

Q: Would the CoSN cyber security planning rubric be an acceptable framework?

In reviewing the COSN cybersecurity plan, it meets the requires of SB 820 identifying risks. Districts would still need to implement mitigation planning.

Q: The definition on the DIR site says "Contractors of state agencies who have access to a state computer system or database must complete training during the term of the contract and during any renewal period." Does that not require all vendors to also complete statewide training requirements?

Per DIR: If the question is whether vendors of local governments have to complete training under HB3834, the answer is no.

Q: Is there is a site that lists all of the Districts Cybersecurity Contacts?

The Cybersecurity Coordinator information is available in the AskTED application. http://mansfield.tea.state.tx.us/tea.askted.web/Forms/Home.aspx

Q: Do you have any recommendations on how to get feedback on our cybersecurity plan without publicly posting it (we consider it to be a confidential doc).

The cybersecurity plan that protects the school districts infrastructure is protected from PIR under
Texas Business Code Section 552.139:

Sec. 552.139. EXCEPTION: CONFIDENTIALITY OF GOVERNMENT INFORMATION RELATED TO SECURITY OR INFRASTRUCTURE ISSUES FOR COMPUTERS. (a) Information is excepted from the requirements of Section 552.021 if it is **information that relates to computer network security**, to **restricted information** under Section 2059.055, **or to the design, operation, or defense of a computer network**.

(b) **The following information is confidential**:

(1) a **computer network vulnerability report**;

(2) any other **assessment of the extent to which data processing operations, a computer, a computer program, network, system, or system interface, or software of a governmental body or of a contractor of a governmental body is vulnerable to unauthorized access or harm**, including an assessment of the extent to which the governmental body's or contractor's electronically stored

information containing sensitive or critical **information is vulnerable to alteration, damage, erasure, or inappropriate use;**

Q: Does DIR have the authority to make that decision for a school district?

Yes, Under Texas Government Code Title 10 Chapter Section 2054.003. DEFINITIONS:

.

(9) "Local government" means a county, municipality, special district, school district, junior college district, or other political subdivision of the state.

Q: IF they self report how will we know who has reported?

Each employee should create their own account on the TxT application. DIR will send a report from TxT to the government body after June 14, 2020 for verification.

Q: Do the employees have to upload evidence of completion?

Per DIR: No

Q: If contractors are coming on campus and utilizing distirct WiFI, will they need to sign a document stating they understand our districts policies?

If contractors are accessing the district WIFI behind the district firewall, they should be signing a nondisclosure agreement and a agreement to comply with district operating policies. If they are only accessing a guest WIFI that gives them access to the only the internet, I would not require them to sign an agreement.

Q: The DIR page is stating that compliance will be reported via the Executive Sign Off Acknowledgement form, unless this doesn't apply to School Districts?

Currently this is only applicable to state agencies.

Q: Do maintenance employees who get a face to face training, have to take a test or can we just include their sign in form.

They should receive a proof of completion at the end of the course.

.

Q: What role do ESCs play in SB820?

The ESC's support the districts by providing assistance such as training. ESC's follow state agency compliance to SB 1597 and file the Texas Cybersecurity Framework wit DIR during even numbered years.

Q: Will there be help desk support for TxT for teachers when having login issues?

Per DIR: Yes, there will be help desk support for Texas by Texas (TxT) website.

Q: Can you give us the gateway url again

Texas Gateway

https://www.texasgateway.org/

Q: Are sample cybersecurity district policies available? Or is there a template district can use to develop their cybersecurity policies/plans?

The cybersecurity policies referred to in SB 820 is a framework which will help the districts protect their infrastructure, identify risk and help with mitigation planning. The Texas Cybersecurity Framework is located at https://www.texasgateway.org/resource/cybersecurity-tips-and-tools ***on the left side under Sections:***

Q: If a teacher moves to another district but was able to complete the training before the deadline, will they have to retake it at the new school employment

Hb3834 requires annual training so if teachers changes schools after the end of the school year, they will be required to complete the certified training for the new district for the next school year. ***Should a teacher move into a new district during the same school year, they would need to take the Certified Security Awareness Training that the new district has chosen as well. If the districts have chosen the same training, when the proof of completion could be used as confirmation.***

Q: is an assessment required? or just requirement to take a security awareness course?

SB820 requires a school district to adopt a cybersecurity policy which does not conflict with the Texas Cybersecurity Framework adopted by Texas state agencies and higher education. The framework will walk you through identifying policies and procedures the district has or needs to implement to protect the sensitive information. Once you have worked through the framework you with be will have benchmark of your current cybersecurity posture and be able to identity risks. You will then be able to develop a mitigation strategy to reduce the identified risks. Working through a framework is similar to a risk assessment.

Q: Do custodians need to be in the training?

Any employee with a login the district network or a district computer is required to take the annual certified training.

Q: do board members of the esc have to take the courses since board directors of the schools have to?

ESC's are considered as state agencies. I would recommend having them take the certified training to have a better understanding of the cybersecurity treats and issues.

Q: are there specific qualifications for the cybersecurity person? Certs?

No specific qualifications have been required for now; however, below is a list of that those interested in getting certified should consider:

CEH (Certified Ethical Hacker)
OSCP (Offensive Security Certified Professional)
CISA (Certified Information Security Auditor)

GCIH (GIAC Certified Incident Handler)
Certified Information Systems Security Professional (CISSP)

Q: Is there way that the superintendent can certify that all employees have been trained rather than each employee having to create an account?

Per DIR's current website: "Local government employees (which school districts) will self-report their training compliance using Texas by Texas (TxT). The expected launch date for this application is February 2020. In June, DIR will send a detailed report from the TxT application to each local government entity to verify training compliance. Although the self-reporting capability will not be available until early February, employees can take their certified cybersecurity training at any time prior to June 14, 2020." The verification process will start after June 14, 2020.

Q: I'm just confused as to where it states the individual staff members are required to report their completion to TxT.

Section B of HB 3834 states:

(b) The governing body of a local government may select the most appropriate cybersecurity training program certified under Section 2054.519 or offered under Section 2054.519(f) for employees of the local government to complete. The governing body shall:
(1) verify and report on the completion of a cybersecurity training program by employees of the local government to the department (DIR)

DIR has determined at this time, TxT is the way that employees will report their completion of the course and after June 14, 2020 DIR will send a report to government body for verification.

Q: What ahout COPPA?

Children's Online Privacy Protection Rule ("COPPA") imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age.

Q: Is there a way to "see" who in the district has self-reported other than the single report in June sent to the superintendent? There has to be a way to mass update and/or send a report with all that have completed the training. Help!

The district should have a list of all of employees who have completed the training for verification.

Q: If there is a breach and no data is compromised do we still need to inform parents about the breach>

There's no requirement to notify the parents if no unauthorized exposure of

student sensitive data occurred.

Q: Again, what would prevent an employee to just say that they got trained without actually being trained? So do they need to upload evidence of completion?

Per DIR: No, local government employees will not need to upload evidence of completion in Texas by Texas (TxT)

Q: What is the Texas By Texas URL for reporting?

The TxT application has not been launched but it is due to be later this month. I suggest you check DIR website: https://dir.texas.gov/View-About-DIR/Information-Security/Pages/Content.aspx?id=154

Q: Do you have the website for Texas by Texas (TxT)? You mentioned it's expected to launch next month. Please advise.

The TxT application has not been launched but it is due to be later this month. I suggest you check DIR website: https://dir.texas.gov/View-About-DIR/Information-Security/Pages/Content.aspx?id=154

Q: Is there a concise list of student PII definitions that will be used by the State of Texas to identify a student information breach?

There is a basic guide for sensitive FERPA and state regulations located at https://www.texasgateway.org/resource/cybersecurity-tips-and-tools on the bottom of the page

Q: Please share the TxT self reporting website?

The TxT application has not been launched but it is due to be later this month. I suggest you check DIR website: https://dir.texas.gov/View-About-DIR/Information-Security/Pages/Content.aspx?id=154

Q: Will we ever get 3rd party contract examples for securing student data and cyber training?

A document has been added to the resources at the bottom of the page entitled: CONTRACT TERMS, CONDITIONS AND AFFIRMATIONS, RESPONSE PREFERENCES AND EXECUTION OF OFFER (Solicitations) at: https://www.texasgateway.org/resource/cybersecurity-tips-and-tools

Q: local gov does not have subcontractor requirement according to HB 3834?

Per DIR: Correct, local government does not have a subcontractor requirement per HB 3834.

Q: Would organizations like uil also need to have verified training? Volunteers, etc handle student data.

The UIL is a part of UT and thus would fall under the state agency definition of compliance. That means anyone who uses a computer more than 25% of the time would have to take the training.

Q: there is a concern that cyber coordinator emails are availble to all public, this was brought up by a school district?

Information in AskTED is available public record.

Q: Is there a list of criteria of specific topics that need to be addressed in our cybersecurity training. I am looking at one of the software options that has been approved. It has training from locking screens to money laundering with over 600 training assets ranging from 1 minute to 5 mintues videos. What amount of training would meet TEA requirements?

HB3834 is an amendment the Texas Government Code and places the Texas Department of the Information Resources (DIR) as the lead agency. TEA isrequired to follow their requirements as well. There is no time limit as part of the criteria. It is based on the content covered.

Q: If a teacher claims they took it at a different district when moving to our district, how will we be able to confirm or deny that with TxT?

The teacher moving into the district would need to take the Certified Security Awareness Training that your district has chosen as well. If the districts have chosen the same training, when the proof of completion could be used as confirmation.

Q: Just to clarify. If the School Board does not have access to a computer system or database they do not have to take the training program. Is this correct?

Per the DIR's current website:
Yes, elected officials are required to complete cybersecurity training regardless of whether they have access to a local government computer system or database.