Question and Answers for Cybersecurity Tips and Tools – Simplifying the Texas Cybersecurity Framework

Session 17

Q: Has DIR came up with an approved list of vendors yet?

DIR has not released a list of certified Security Awareness Training vendors. They anticipate the first release by the of end October.

Q: Should the cybersecurity policy be posted in the Board "CQ" policies of districts or is there another division it should be posted in?

I recommend the cybersecurity policy be located with your Disaster Recovery Plan or Multi Hazard Plan.

Q: Will the revised Framework be updated on the Texas Gateway site?

The 2020 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 can I get the new Texas CSF and has it been mapped to NIST, CIS, and other frameworks?
The 2020 Texas Cybersecurity Framework (TCF) self-assessment spreadsheet can be found at https://www.texasgateway.org/resource/cybersecurity-tips-and-tools under Texas Cybersecurity Framework. On the roadmap tab, the TCF is mapped to the NIST framework.

Q: What is the limit between the functions "Respond" and "Recover"? May recovering be a part of responding.

Yes, Respond and Recover work hand in hand. When you detect an anomaly, you start the respond function. Depending on what is uncovered in the Respond (for example a false/positive) you may move directly to the Recovery stage or close the incident.

Q: When will the Texas Cybersecurity Framework on the Texas Gateway be updated with the latest additions to Identify, Protect and Detect?

The 2020 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 TEA template for vendors that districts can use? This has been mentioned for the past 2 school years.

School districts can use any framework for the cybersecurity policy which does not conflict with the Texas Cybersecurity Framework. The 2020 Texas Cybersecurity Framework self-assessment spreadsheet can be found at https://www.texasgateway.org/resource/cybersecurity-tips-and-tools under Texas Cybersecurity Framework. The Texas Cybersecurity framework can be used as a template.

Q: Is there an estimated time for us to start seeing certified programs?

DIR has not released a list of certified Security Awareness Training vendors. They anticipate the first release by the end of October.

Q: The Texas Gateway only has a sample file of a few of the roadmap objectives. Where can we get a full listing?

The 2020 Texas Cybersecurity Framework self-assessment spreadsheet can be found at https://www.texasgateway.org/resource/cybersecurity-tips-and-tools under Texas Cybersecurity Framework. The 2020 Texas Cybersecurity Framework includes a tab containing all 46 objectives with sample ratings and the graphic to assist in indicating risks. There is a tab with a sample for tracking your security posture of time and tab with definitions for all 46 objectives with mappings to the NIST framework as well as a roadmap with recommendations for each objective to reach a 3.0 rating level.

Q: Thoughts on an auditing/compliance/data classification solution?

There are several tools out in the market for auditing/compliance solutions. Data classification requires some input as to what each district may want to classify as sensitive or protected information. On the Texas Gateway at the bottom of the website, there is a Related Items section. A Sensitive Information Guide is available to identify federally and state regulated information: https://d18n8r6t2iitwf.cloudfront.net/resources/documents/Sensitive%20information%20guides-%20TEAv2.docx

Q: Can you talk a little about what Redbook is?

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.

The Redbook is a template which contains information on federal and state regulations and information on what actions need to be taken during the Response and Recovery functions. It is provided in a Word document format so it can be modified to include your incident response team and incident reporting through your level of management.

Q: Can we use the CIS control as well?

ISD's may chose other frameworks which will protect the district's 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 in 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. The CIS CAT Lite (Center for Internet Security® Configuration Assessment Tool) https://www.cisecurity.org/blog/introducing-cis-cat-lite/ can also be used to meet the SB820 requirements.

Q: This is an overwhelming process for a small rural district with limited staff. It is nice to have you and the gateway site as a resource. But it is still daunting

I agree. Both TEA and the ESC's use the Texas Cybersecurity Framework and want to help the school districts through this process.

Q: Can you go back to the slide with URL's while you answer questions?

The presentation slides and the video recording are posted at https://www.texasgateway.org/resource/cybersecurity-tips-and-tools

Q: Can you make comparison between the NIST CSF framework and the ISO3100 Standard and also the Information Security Management System (ISMS). What are the similarities and differences between them?

I have provided a crosswalk reference guide to compare some of the common frameworks in the Related Items sections at the bottom of the Texas Gateway

Question and Answers for Cybersecurity Tips and Tools – Simplifying the Texas Cybersecurity Framework

Session 17

website:https://d18n8r6t2iitwf.cloudfront.net/resources/documents/Copy%20of%20Crosswalk%20of%20Texas%20Cybersecurity%20Framework%20compared%20to%20other%20frameworks.xlsx

Q: What if a vendor is unable or unwilling for their security to answer some of these questions regarding backup locations, or other matters?

Most vendors are willing to provide this type of information. Vendors not able to provide this type of information regarding how and where they store your information, may need to be removed from your potential vendor list.

Q: Has AskTed been updated to input the Cybersecurity Point of Contact?

Yes, AskTed has been updated and school districts can designate the cybersecurity coordinator.

Q: How do we enter our cyber security coordinator on ASKTed?

After the superintendent or designee logs in to AskTed, navigate to the District Personnel tab. Under District Central Office Personnel Listing, click Add Personnel. Add the First name, Middle name and Last name and select the Cybersecurity Coordinator from the Roles: list. Add the Phone number, Fax number and Public Email Address then check the Use District's Address and SAVE.

Q: Question: If we have a dedicated Cyber Officer, how long can we expect for DIR to certify our training program?

DIR has not released a list of certified Security Awareness Training vendors. They anticipate the first release by the of end October.

Q: HB3834 allows self-created training as well correct. 3rd party is not required correct?

Per HB3834, "a local government that employs a dedicated information resources cybersecurity officer may offer to its employees a cybersecurity training program that satisfies the requirements". The self-created training is required to be submitted to DIR for review.

Q: When will the slide deck and recording of this session be available?

Question and Answers for Cybersecurity Tips and Tools – Simplifying the Texas Cybersecurity Framework

Session 17

Both the slide deck and the recording of all the webinars and Question and Answers have been posted at https://www.texasgateway.org/resource/cybersecurity-tips-and-tools

Q: How do we create a consortium to help drive vendor costs down on security products?

In many case's the ESC's have negotiated discounted pricing for security products. The Texas Department of Information Resources (DIR) has also negotiated contracts a school district can take advantage of.

Q: If we implement an Employee Awareness Program through a vendor to do phishing tests and cybersecurity training, does that vendor must be approved by DIR? Or are we free to go ahead and choose a vendor without them being on the approved vendor list?

All local governments are required under HB3834 to provide security awareness training to all employees with access to a local government computer, including elected officials, on an annual basis. The training must have been certified by DIR and an annual report submitted to DIR of the employees required to take and who have taken the training.

Q: Thank you!