Question and Answers from the 2019-09-04 Cybersecurity Tips and Tools – Ransomware Prevention, Detection, and Recovery

Q: will you be sending recording url?

Yes, the webinar and presentation slides have been uploaded to https://www.texasgateway.org/resource/cybersecurity-tips-and-tools

Q: How exactly does each superintendent designate a cybersecurity coordinator to TEA?

The district Superintendent or designee can add the role of Cybersecurity Coordinator in ASKTED under District Administration/Organization/District Personnel.

Q: Regarding the slide "To Pay or Not to Pay", you mention 40% have been paying, a) what is the general recommendation and b) what are the pros/cons of both approaches?

The decision is based on your organization's ability to wipe, rebuild and restore from backups in a timely matter.

Q: This is regarding the RedHat handbook that was mentioned - where is this located?

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: Can we get a list of regional FBI contacts for cyber security issues?

Texas has three FBI field offices:
Dallas (972) 559-5000, Houston (713) 693-5000 and San Antonio (210) 225-6741

Q: When will ESCs be assigned an FBI contact?

We plan to have that completed by November.

Q: You mentioned the Texas Cybersecurity Framework, the one with the 40 points, being housed at a website. Is there a direct link to it?

https://www.texasgateway.org/resource/cybersecurity-tips-and-tools at the bottom of the website Related Items/Documents

Q: Is there a threshold in regards to a certain number/amount of devices infected before we have to report it to TEA?

SB820 requires school districts to report any "breach of system security" - an incident in which student information that is sensitive, protected, or confidential, as provided by state or federal law, is stolen or copied, transmitted, viewed, or used by a person unauthorized to engage in that action. So, whether it involves one computer or all of systems, school districts are required to report it to TEA. We recommend you contact us anytime you suspect you have an incident, so we have order avenues of assistance. Please contact TEA at: ***cybersecurity@tea.texas.gov***

Q: Was TEA impacted directly by the Ransomware attack you mentioned at the beginning?

No, TEA has not been impacted by ransomware, yet.

Q: can you share Jordan's contact information?

No, I would recommend contacting the FBI through one of the three field offices in Texas:Dallas (972) 559-5000, Houston (713) 693-5000 and San Antonio (210) 225-6741

Q: IS K12 one of the higher trending industries with more cyber attacks?

Yes, due to student data having one of the highest values on the Dark Internet. Student data can be misused for years before it is detected as they enter the work force, military on higher education.

Q: Have the authorities ever caught the perpetrators of a ransonware attack?

Yes, perpetrators are often caught if the right law enforcement is engaged early in the discovery process. I recommend disconnecting all Wired and Wireless network connections but do not turn off the infected computers until a forensic analyst or law enforcement can analyze and dump the memory. If it is shut down, what's in memory is lost.

Q: It appears that these threats/attacks come in waves and specific industries were given a heads up in regards to the recent rash of ransomware attacks. Can school districts start getting heads up for these type of attacks as well? Or is there a location that we can go to see threat levels?

Below are a few websites I find helpful:
The Multi-State Information Sharing & Analysis Center (MS-ISAC)
https://www.cisecurity.org/ms-isac/
The Internet Storm Center https://isc.sans.edu
SANS NewsBites https://www.sans.org/newsletters/newsbites

Q: when will it be ready for the supers to do that within ASK TED?

The update for AskTED to add the Cybersecurity role was implemented into production on 9/13.

Q: May have missed this...you talked about free training resources?

There are a couple of free training resources listed on the Cybersecurity Tips and Tools portal:
https://www.texasgateway.org/resource/cybersecurity-tips-and-tools

1) *https://www.cybrary.it/*
2) *Department of Homeland Security - The Federal Virtual Training Environment (FedVTE) is a free, online, on-demand cybersecurity training system managed by DHS that is available to federal and SLTT government personnel, veterans, and federal government contractors, and contains more than 800 hours of training on topics such as ethical hacking, surveillance, risk management, and malware analysis.*
   https://niccs.us-cert.gov/training/federal-virtual-training-environment-fedvte

Q: Is there a form or an expected format to use when contacting TEA regarding a qualified event under SB820

Most importantly, contact us as soon as possible. We can help identify resources and provide guidance. As we assist in the process, we will be able to determine what the cyber threat is, when it occurred, what actions are you taking and work with you on lessons learned. As part of the lessons learned, determine the estimated number of man hours (resources) used to identify and mitigate the situation.

Q: encourage people to join their local InfraGard chapter to connect with FBI

Infragard is a partnership between the FBI and members of the private sector. Infragard provides a vehicle for seamless public-private collaboration with government that expedites the timely exchange of information and promotes mutual learning opportunities. More information on Infragard is located at: https://www.infragard.org/

As ESC staff, if a school reports to us an event, should we report to TEA/DIR as well on the school's behalf?

Yes, I recommend the ESC's reaching out to TEA as well once they are notified. The school district impacted may have their hands full with performing Incident Response. TEA will also notify the ESC to see if they are aware of the situation.

Q: Does that mean they will need an SSN, or can they also practice ID theft without the SSN?

Identity thief can involve the use of a SSN but also involve credit theft, establishing new accounts under your name to cover some of the issues involved with identify theft.

Q: What is the latest DIR Redbook date?

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 was the name of the org ic3 Org?

*The Internet and Computing Core (**IC3**) **Digital Literacy** Certification tests basic **computer** skills and understanding of the Internet to promote success in school, work and life. CCI Learning is the world's leading courseware developer for **IC3**. More information can be found at: https://certiport.pearsonvue.com/Certifications/IC3/Digital-Literacy-Certification/Overview*

Q: Would you provide some sort of guidance on the cyber security liability insurance

There are several sources for cybersecurity insurance. Please check to make sure what the policy covers and what action you need to take in a cybersecurity incident for the policy to pay out.

Q: this seems like a full time job what are small school districts supposed to do to prepare when there is one person managing everything this is almost sounding impossible.

Yes, it can seem overwhelming; however, working in collaboration with each other and the ESC's we can get this done. Cybersecurity is not a weekend trip, it is journey. We simply need to learn how to identify risks and establish priorities to mitigate them to protect our infrastructure and the information which has been shared with us..

Q: where was it communicated that cyber coordinator needed to be reported on askted? can you provide a refrence link?

In SB820 it states, "each school district shall designate a cybersecurity coordinator to serve as a liaison between the district and the agency in cybersecurity matters." TEA will need to be able to identify who each district has designated. For example, we plan to notify all the Cybersecurity Coordinators of future webinars directly. TEA has chosen AskTED as the best method to collect the information required in the legislation.

Q: Thanks for everything Frosty. Take care.
Q: Thank you! Great webinar!! Very informative!