Questions and Answer Session for Monday March 23rd -- Cybersecurity Challenges Working with a Remote Workforce

Q: Can you share what VPN services are recommended?

VPN services may depend on the brand of firewall you are using. It is recommended to check with your firewall vendor to see what VPN services are supported by your firewall.

Q: Can I use VPN with IPSec for an employee's personal computer for remote users?
It is not recommended to connect VPN services to a personal owned device, as the security of the device is not managed by the school district. For users with a personal owned device, it would be recommended to consider a virtual desktop solution if applicable.

Q: Should student emails for Google classroom be considered sensitive?

It depends. If your district has defined FERPA directory information and email is included, the email is not considered sensitive information unless the parents have opted out of sharing directory information, in which case, it becomes protected sensitive information.

Q: Will there be a video of the webinar after?

Yes. The video of the webinar and the presentation slides was made available on March 25th at the link below. Below is a link to the Texas gateway portal where all the webinars and cybersecurity resources have been shared:

https://www.texasgateway.org/resource/cybersecurity-tips-and-tools

Q: What is the HB 3834 2020 deadline? Is it still required by June 14th or has it been postponed? It will be next to impossible to get this done in the current environment.

Below is DIR's response as of March 25th:

For now, it is best to assume that a compliance date will remain in effect unless otherwise notified. DIR is aware of reporting and compliance deadlines over the upcoming few months and the challenges some organizations may have in meeting those deadlines. Most of these deadlines are set in statute and therefore DIR does not have the authority to delay or reschedule submission deadlines. Regarding the cyber training requirements of HB 3834, it is imperative – now more than ever with an increased remote work force – that all public sector employees are as prepared as possible to work securely with heightened awareness for cyber threats. Because of this, each organization should continue to make cyber training a high priority. Low and no-cost certified training programs have been available on DIR's website since October 2019 (see:

https://dir.texas.gov/View-About-DIR/Information-Security/Pages/Content.aspx?id=154#list) and all public sector employees are strongly encouraged to complete the required training utilizing one of these certified programs. For organizations required to report compliance, DIR will provide an online form for attestation of compliance in April 2020.

Q: What is the most secure remote access software recommended?

If the district owns the PC and it has been authenticated on your network, there should not be an issue if you have automatic updates for OS and AV patching. Remember VPN services, typically create a virtual private tunnel between the end user and your firewall. This can be a cybersecurity issue when dealing with Bring Your Own Device (BYOD) if you do not have the ability to sandbox the end user to check for the latest AV signatures and OS patches. With VPN and BYOD, you can easily introduce malware from the BYOD directly behind your firewall. For BYOD users, it is suggested to use a virtual desktop solution.

Q: Are there any free antivirus programs that we can offer to employees using personal devices?

There are several free antivirus (AV) programs available, but it is recommended that due diligence research is performed before deploying any free AV programs. Best practice would be to use a well-known AV program as it is a major part of our protection strategy.

Q: I am receiving communication from MS-ISAC and hearing reports of Distributed Denial of Service (DDOS) incidents against school districts. Do you have any information regarding that?

DDOS attacks are a common threat. TEA has not received a report of one from a Texas K-12 since the beginning of the year. However, schools are not required to report this type of attack to TEA currently.

Q: Any thoughts on teachers using Zoom to meet with their students?

Zoom is one of many viable applications to conduct video conferencing, including meeting with students. Refer to vendor's recommendation for best practice on security configurations.

Q: Are you aware of any Security Awareness training courses specific to remote working or COVID-19?

 The Texas Department of Information Resources has posted some good information at:
https://dir.texas.gov/View-Resources/Pages/Content.aspx?id=69

Q: Where can districts get free hotspots?

It is recommended that you check with your ESC, as they may have a better idea of free services being offered in your region.

Q: With an anti-virus filter, email filter and secure VPN, what else is the next thing that is recommended?

You have the basics. You may want to consider an additional endpoint solution or cloud application monitoring solution.

Q: Is there a cybersecurity email template that can be shared to send to our staff?

We do not have an email template, however we suggest including these recommendations in your communication:
- ***Before entering your UserID credentials on any website, make sure the URL displayed is a valid URL.***
- ***Examine links in emails by hovering over them before clicking (look for expected URLs).***
- ***Examine the From field and the email address displayed (look for @school.isd.net or known business partners).***
- ***Be extra suspicious about phone #'s included in emails. (Use a known good phone # to verify the originality of the sender.)***
- ***Don't open attachments if you are not certain of the sender and the content.***
- ***When Windows Updates are available, install them immediately for all security & critical patches.***
- ***Forward questionable emails that make it to your Inbox (not the Junk folder) to a security helpdesk for review.***

Q: Who is providing free internet?

It is recommended that you check with your ESC as they may have a better idea of free services being offered in your region.

Q: Please provide the links for remote VPN setup for employee home PCs to company server access.

SANS has a WFH deployment guide that might be helpful:
https://www.sans.org/security-awareness-training/sans-security-awareness-work-home-deployment-kit

Q: Are HB 3834 Open Enrollment Charter schools exempt?

Yes, Charter Schools are exempt. They are not included in the Texas Government Code definition of local government:

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.