Cybersecurity Tips and Tools – Cybersecurity Challenges with a Remote Workforce

Frosty Walker and Melinda Dade

Chief Information Security Officer

Texas Education Agency

cybersecurity@tea.texas.gov

Data Security Advisory Committee

The Data Security Advisory Committee (DSAC) provides guidance to the Texas education communities, maximizing collaboration and communication regarding information security issues and resources which can be utilized within the educational communities served.

The DSAC is currently comprised of representatives from school districts, ESCs, TEA and the private sector.

Texas Gateway

https://www.texasgateway.org/

Cybersecurity Tips and Tools

Currently under Maintenance
Due back in Service March 25th

Cybersecurity Challenges with a Remote Workforce

- Schools must understand and address the challenges associated with a mobile workforce.
- Even large districts with multi-million dollar budgets face difficulties managing a remote workforce.
- The challenge is bigger for smaller districts that need to work with limited budgets.
- Working with remote employees demands that schools pay acute attention to the technology and security they use.

Reduced Security on BYOD and Mobile Devices

- Cybersecurity is no longer just a challenge. It is a constant threat. In a landscape like this, complexity is doubled when data moves outside the confines of the office.
- When employees work remotely, they often use personal devices and public Wi-Fi networks, which can expose your important data to several other vulnerabilities. This poses a major threat to data security.
- Clearly, data security is a huge liability with remote employees—one that needs to be dealt with as a top priority.

Have a Plan and Operating Policy for Telework

1. **Eligibility -** who is eligible
2. **Availability -** establish schedule guidelines
3. **Responsiveness -** implement specific rules for response time
4. **Productivity measurements -** establish how an employee's productivity will be measured
5. **Equipment -** establish guidelines for equipment standards (BYOD)
6. **Physical environment -** establish and approve remote location
7. **Security and confidentiality -** establish security guidelines, (i.e. no public Wi-Fi, current AV, handling PII)

Address Data Security Issues

- Increase awareness about security and sensitize their remote workers, and educate them about the possible dangers and preventive best practices.
- Strict password policies should be enforced.
- Employees should be required to secure the laptops they intend to use for work (BYOD).
- Schools can designate a remote employee’s work device and secure it themselves with authorized antivirus and security software.

Tracking and Managing Assets

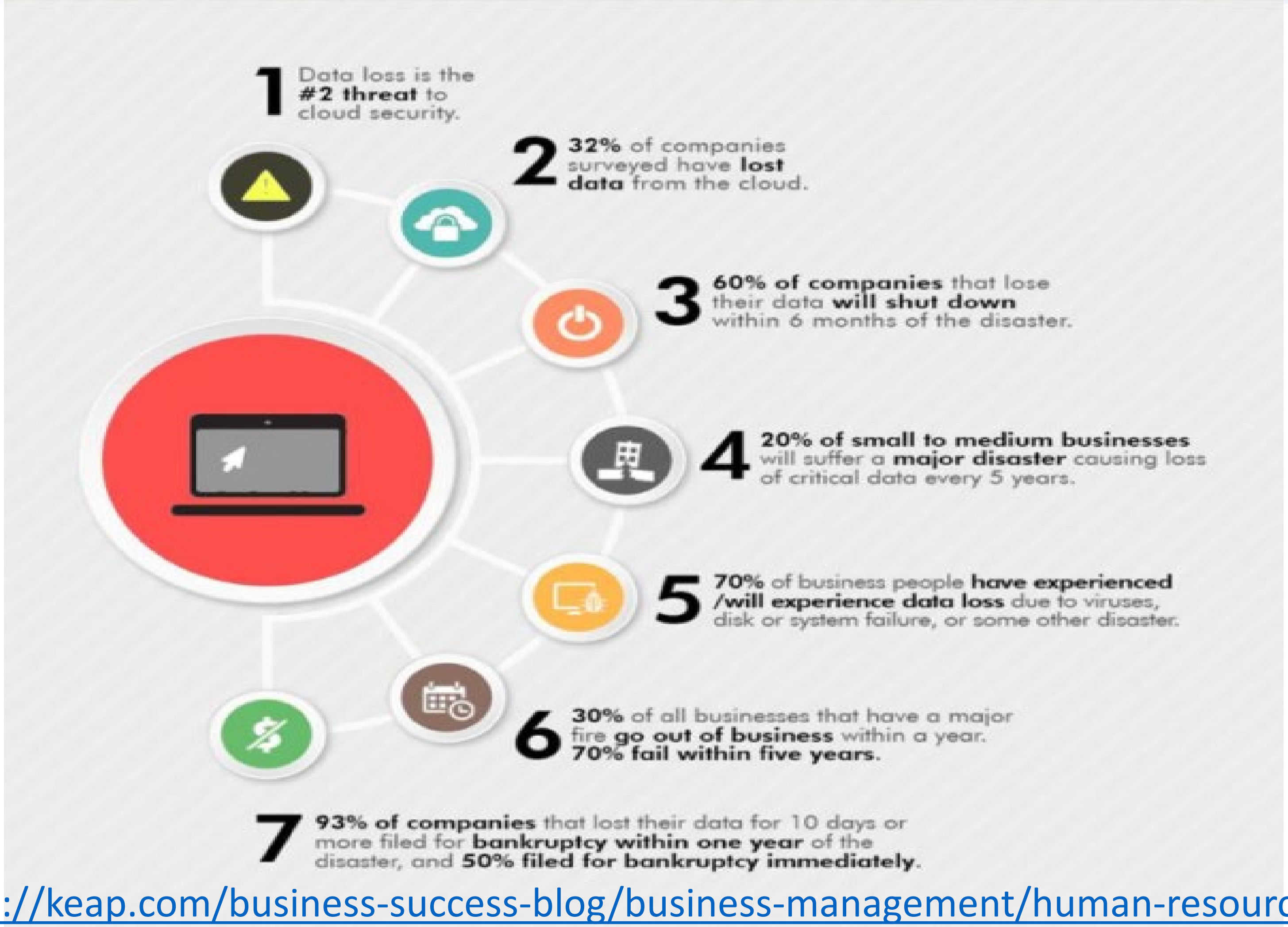
- Protecting and managing all such assets should be a major priority for any school.
- Using solutions such as **Data Loss Prevention (DLP), geofencing**, **predictive asset monitoring**, and **ticketing systems** can help schools better handle their asset management needs.
- Use Virtual Private Networking (VPN) for school owned devices deployed remotely that need remote access.
- Use a remote access software such as Citrix for users with personal devices that need remote access.

Inadequate Backup and Recovery Systems

- In case of an accidental data loss, remote employees using their own devices often do not have adequate backup and recovery options.

- The problem becomes even more pronounced when your remote employees use the same device for work as well as personal use, often mixing up personal and school data, exposing each to the vulnerabilities of the other.

Statistics about Data Loss



1 Data loss is the **#2 threat** to cloud security.

2 **32%** of companies surveyed have **lost data** from the cloud.

3 **60% of companies** that lose their data **will shut down** within 6 months of the disaster.

4 **20% of small to medium businesses** will suffer a **major disaster** causing loss of critical data every 5 years.

5 **70%** of business people **have experienced /will experience data loss** due to viruses, disk or system failure, or some other disaster.

6 **30%** of all businesses that have a major fire **go out of business** within a year. **70% fail within five years.**

7 **93% of companies** that lost their data for 10 days or more filed for **bankruptcy within one year** of the disaster, and **50% filed for bankruptcy immediately.**

SOURCE: https://keap.com/business-success-blog/business-management/human-resources/security-challenges-for-remote-businesses

Addressing Appropriate Backups and Recovery

- Employees can have a local backup on their laptops or personal device.
- Consider providing them a centralized data backup and recovery program for all remote devices carrying crucial school data.
- Plenty of SaaS providers offer cloud backup solutions customized for schools, and effectively cover your backup needs for the office as well as remote employees in one single account, eliminating all hassle and keeping all your data secure in case of any crashes, lost devices or other problems.

Sensitizing Employees to Follow Data-Security Protocols

- Face-to-face communication beats every texting technology out there, regardless of its cutting-edge abilities. Email, WhatsApp, Telegram are all excellent messaging methods, but they're no match for good old-fashioned, face-to-face conversations when you want to convey your message, especially when speaking of highly sensitive issues, such as your school's data security.
- When dealing with remote teams, you're obviously faced with the challenge of not being able to sit in the same room with your employees. In this case, it's best to go to the next solution in line: video conferencing such as **Zoom** or **GoToWebinar.**

Wrapping It Up

- We have covered some of the major challenges that we face when dealing with borderless workforces and employees who access information on their personal devices.
- Now that you know some of the challenges, buckle up and fight it out.
- Invest in security; it might just be the best investment you can make.
- Sensitize your remote workforce about the above challenges and get them to join in the fight to make telecommuting a bigger success.

Here are some important tips to safeguard your users:

- 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.)

Here are some important tips to safeguard your users:

- 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.
- Reference Operating Policies (such as Acceptable Use and Cloud Computing Policies and Telework Policies) as a reminder to your users

Here are some important tips to safeguard your users:

Remind remote access users their responsibility for exercising reasonable care in ensuring the security of the non-school equipment being used. At a minimum, the user will ensure that the following safeguards and practices are in place:

(1) The computer or mobile device used for remote access is equipped with a supported, up-to-date operating system utilizing fully patched software.

(2) No other people are allowed physical or networked access to the computer or mobile device while it is being used to access school information resources.

(3) Extending the school network to a third-party network is unauthorized.

Texas Education Agency

Here are some important tips to safeguard your users:

(4) The computer or mobile device is being physically secured even when it is not in use (i.e., in a securely locked home or office).

(5) Any PII data should be encrypted in transit and at rest

(6) The computer or mobile device is secured with password or biometric protection restricting access to the operating system.

(7) No confidential, proprietary or access-related data is downloaded to or stored on the local computer or mobile device without the use of approved encryption.

(8) Any known security compromise of the local computer or mobile device is immediately reported to your Information Security Team.

Additional Resources

Texas Education Agency (TEA)

https://tea.texas.gov/texas-schools/safe-and-healthy-schools/coronavirus-covid-19-support-and-guidance

Texas Department of Information Resources (DIR)

https://dir.texas.gov/View-Resources/Pages/Content.aspx?id=69

Consortium of School Networking (COSN)

https://www.cosn.org/sites/default/files/COVID-19%20%26%20Cybersecurity%20-%20Member%20Exclusive.pdf

Questions?

Questions regarding HB3834

Texas DIR website:

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

TEA

Texas Education Agency

Thank you!