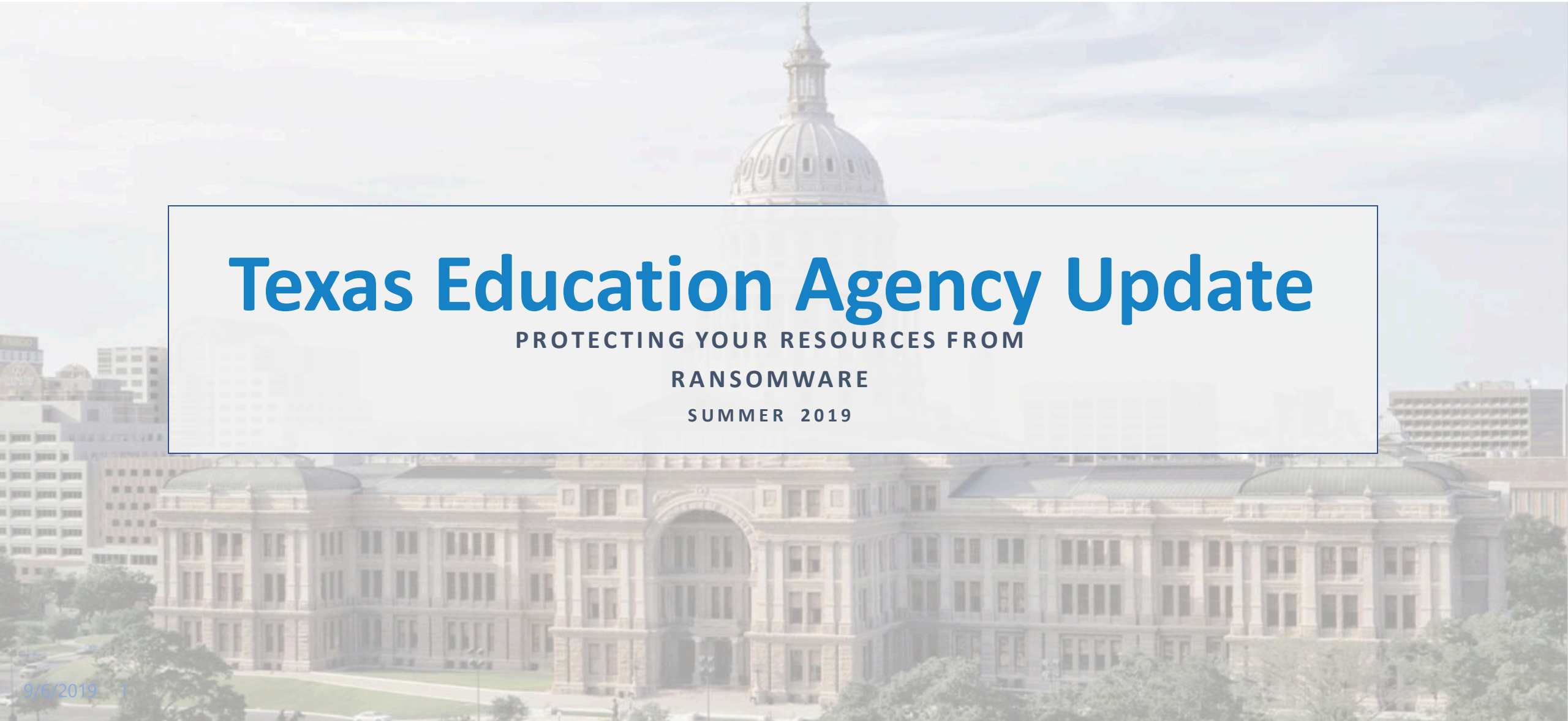

Texas Education Agency Update

PROTECTING YOUR RESOURCES FROM RANSOMWARE

SUMMER 2019

Ransomware

Texas Gateway

https://www.texasgateway.org

Cybersecurity Tips and Tools

Ransomware

Ransomware Attacks on Businesses Are Skyrocketing

Florida City Paying $600,000 to End Ransomware Attack

Over 20 Texas local governments hit in a coordinated ransomware attack

Hackers Are Holding Baltimore Hostage: How They Struck and What's Next

Ransomware attack sends City of Del Rio back to the days of pen and paper

Servers at City Hall were rendered useless due to the outbreak.

Ransomware

** source:* https://www.google.com/maps/d/viewer?mid=1UE6Nko9iRG1tLci_AeqqsxzxGzs&ll=40.75531828029828%2C-112.87596879221996&z=4

Ransomware

- **Ransomware is a type of malicious software,** or malware, designed to deny access to a computer system or data until a ransom is paid. *
- **Ransomware typically spreads through phishing emails** or by unknowingly visiting an infected website.*
- No organization is immune to an attack. **Government organizations and medical facilities who retain large amounts of sensitive information** and need access to those files immediately are enticing targets as they are more likely to pay to have the data restored.

** source: https://www.us-cert.gov/Ransomware*

Ransomware

- Ransomware has been the most pervasive cyber threat since 2005. According to publicly available information, ransomware infections have outnumbered data breaches over the past 11 years.*

- The cybersecurity research body suggests that ransomware damage costs will rise to $11.5 billion in 2019. **

- It is a lucrative business for cybercriminals and will continue to grow as there is value is encrypting and restricting access to user's data.

* *source:* https://www.csoonline.com/article/3095956/the-history-of-ransomware.html#slide1

** *source:* https://phoenixnap.com/blog/ransomware-statistics-facts

Types of Ransomware

Types of Ransomware and their effects

- **Most Common Types:**
  - **Crypto –used to encrypt the files or data preventing access**
  - **Lockers-used to lock the computer or device**

- **Other Types:**
  - **Scareware- claims to find issues on your computer and will resolve them for money**
  - **Doxware- threatens to publish your information if you don't pay ransom**
  - **RaaS- ransomware as a service hosted anonymously by hackers**

- **What do these types all have in common?**
  - **They hijack your data and won't allow you access till you pay a fee!**

Do’s and Don’ts

Dos of Ransomware

- Do have a proactive cybersecurity framework plan.
- Do backup your systems and files and verify that they are backed up.
- Do store backups separately and offsite.
- Do update software and operating systems with the latest patches.
- Do train your employees.

Don’ts of Ransomware

- **Don’t automatically open email attachments.**
- **Don’t provide personal or financial information via email, unsolicited phone call, text message or instant message.**
- **Don’t provide personal or financial information about your organization via email, unsolicited phone call, text message or instant message.**
- **Don’t allow users to install and run software applying the least privilege.**

Prevention and Detection

Prevention and Detection

- **Run Frequent Scheduled Security Scans.**
  - All the security software on your system does no good if you are not running scans on your computers and mobile devices regularly.
  - These scans are your second layer of defense in the security software.
  - They detect threats that your real-time checker may not be able to find.

- **Enforce Strong Password Security**
  - Utilize a password management strategy that incorporates an enterprise password manager and best practices of password security.

- **Segment your network.**
  - Limit the data an attacker can access.
  - With dynamic control access, you help ensure that your entire network security is not compromised in a single attack.
  - Segregate your network into distinct zones each requiring different credentials.

Source:https://phoenixnap.com/blog/enterprise-password-management-solutions

Prevention and Detection

- **Employ content scanning and filtering on your mail servers.**
  - Inbound e-mails should be scanned for known threats and should block any attachment types that could pose a threat.(*.exe)

- **Use reputable antivirus software and a firewall.**
  - Maintaining a strong firewall and keeping your security software up to date are critical.
  - It's important to use antivirus software from a reputable company because of all the fake software out there. Many AV's now include ransomware detection.

- **Educate your staff**
  - Provide Security Awareness Training on best practices

Removal

Removal of Ransomware

➢ Contact your IT support team and IT security team

- They will remove the malware from the device but note your files have already been encrypted and it will be impossible to unlock them without the key.
  - Per requirements of SB 820, 86th Regular Session, school districts are required to report incidents to TEA.
  - School districts should also alert their ESC and the FBI.

➢ Isolate the infected device/system

- Remove the infected system from all networks, and disable the computer's wireless, Bluetooth, and any other potential networking capabilities. Ensure all shared and networked drives are disconnected whether wired or wireless.

➢ Secure backups

- Ensure that your backup data is offline and secure. If possible, scan your backup data with an antivirus program to check that it is free of malware.

Source: https://www.us-cert.gov/ncas/tips/ST19-001

Recovery

Ransomware recovery

- By planning for cyber resilience and maintaining offsite, back-up servers, agencies and organizations can recover from attacks more quickly.*
- Revisit your Cybersecurity plans making any necessary updates, ensuring that critical infrastructure is protected.
- Prevention is the most effective approach rather than trying to treat the systems!

*Source: https://urbancyberdefense.mit.edu/blog/Data-Recovery-Firms-Add-New-Layer-Complexity-Ransomware-Decisions

To pay or not to pay?

To pay or not to pay?

- Nearly 40 percent of ransomware victims paid the ransom. (*Source:* Malwarebytes)

- The Baltimore City government was hit with a massive ransomware attack in 2019 that left it crippled for over a month, with a loss value of over $18 million. (*Source*: Baltimore Sun)

- After getting hit by the SamSam ransomware in March 2018, Atlanta, Georgia, has spent more than $5 million rebuilding its computer network, including spending nearly $3 million hiring emergency consultants and crisis managers. (*Source:* Statescoop)

- A Massachusetts school district paid $10,000 in Bitcoin after a ransomware attack in April 2018. (*Source*: Cyberscoop)

To pay or not to pay?

- **This is a decision that must be made by each organization on a case by case basis.**
- **While regaining control of your data is the ultimate objective, please consider the following:**
  - The FBI discourages agencies/organizations from paying the ransom as this encourages future attacks.
  - Paying the ransom does not guarantee you will get your files back in a useable form. The expense is usually not in paying the ransom, but in recovering and rebuilding the files.

- **Taking preventative measures and having a proactive cybersecurity plan is the key to preventing a ransomware attack!**

Upcoming Cybersecurity Webinars

Upcoming Cybersecurity Webinars

Date/Time	Cybersecurity Tips and Tools – SB 820 and HB 3834 (86th) Impact and Requirements to Texas School Districts
Wednesday, September 11, 2019 **1:00 pm –2:00 pm CDT** **Webinar Registration** **https://attendee.gotowebinar.com/register/6410737030503214860**	The September 11th webinar provides information on SB 820 and HB 3834 and their potential impacts for Texas school districts. The presentation will include planned processes to address the requirements established by the bills' amendments to the Texas Education Code and Government Code. Superintendents, cybersecurity coordinators and representatives interested in cybersecurity issues and resources, which can be utilized within the education communities, are encouraged to attend.

Upcoming Cybersecurity Webinars

Date/Time	Cybersecurity Tips and Tools – Simplifying the Texas Cybersecurity Framework
Wednesday, October 2, 2019 **1:00 pm –2:00 pm CDT** **Webinar Registration** **https://attendee.gotowebinar.com/register/8734738474448037131**	The October 2nd webinar will cover the Texas Cybersecurity Framework (TCF) and its primary function. This presentation provides information on the fundamental categories of Identify, Protect, Detect, Respond and Recover, which are incorporated into the TCF. The TCF meets the requirements for the cybersecurity policy in SB 820. Understanding the categories and the objectives for each can be beneficial to your end users and assist your organization in complying with SB 820. Cybersecurity coordinators and representatives interested in information security issues and resources, which can be utilized within the education communities, are encouraged to attend.

Upcoming Cybersecurity Webinars

Date/Time	Cybersecurity Tips and Tools – Basic Incident Response
Wednesday, November 6, 2019 **1:00 pm –2:00 pm CST** **Webinar Registration** **https://attendee.gotowebinar.com/register/6955238278520376331**	The November 6th webinar provides information regarding Basic Incident Response and the impact of a cybersecurity incident for your organization. This presentation will cover fundamental steps your organization will need to perform when a cyber event becomes an incident. Understanding the Basic Incident Response fundamentals with help cybersecurity coordinators being compliant with SB 820 requirements in reporting a breach of system security Cybersecurity coordinators and representatives interested in information security issues and resources, which can be utilized within the education communities, are encouraged to attend.

Resources

- Department of Information Resources http://dir.texas.gov/
- Texas Education Agency https://tea.texas.gov/Home/
- Cybersecurity Tips and Tools https://www.texasgateway.org/node/153181
- Cybersecurity and Infrastructure Security Agency (CISA) https://www.us-cert.gov/Ransomware
- National Institute of Standards and Technology https://www.nist.gov/cyberframework
- National Institute of Standards and Technology Guide to Cybersecurity Event Recovery https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf