Information Security Forum
Cybersecurity Updates
03/10/2020

Frosty Walker

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

SB 820

) Each school district shall adopt a cybersecurity policy to:

- (1) Secure district cyberinfrastructure against cyber-attacks and other cybersecurity incidents
- (2) Determine cybersecurity risk and implement mitigation planning
- (3) Designate a Cybersecurity Coordinator
- (4) Report a “breach of system security” to TEA
- (5) Notify parents of breach of protected student information

(c) School district’s cybersecurity policy may not conflict with the information security standards for institutions of higher education adopted by the Department of Information Resources under Chapters 2054 and 2059, Government Code. (Texas Cybersecurity Framework)

SB 820

d) The superintendent of each school district shall designate a cybersecurity coordinator to serve as a liaison between the district and the agency in cybersecurity matters. (in the AskTED application)

(e) The district ’s cybersecurity coordinator shall report to the agency any cyber-attack or other cybersecurity incident against the district cyberinfrastructure that constitutes a breach of system security as soon as practicable after the discovery of the attack or incident.

(1)“ Breach of system security" means 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.

SB 820

(f) The district ’s cybersecurity coordinator shall provide notice to a parent of or person standing in parental relation to a student enrolled in the district of an attack or incident for which a report is required under Subsection (e) involving the student ’s information.

SB 820 Enforcement

TEA may enforce this provision of the Texas Education Code, section 11.175, through special accreditation investigations pursuant to section 39.057(a)(16).

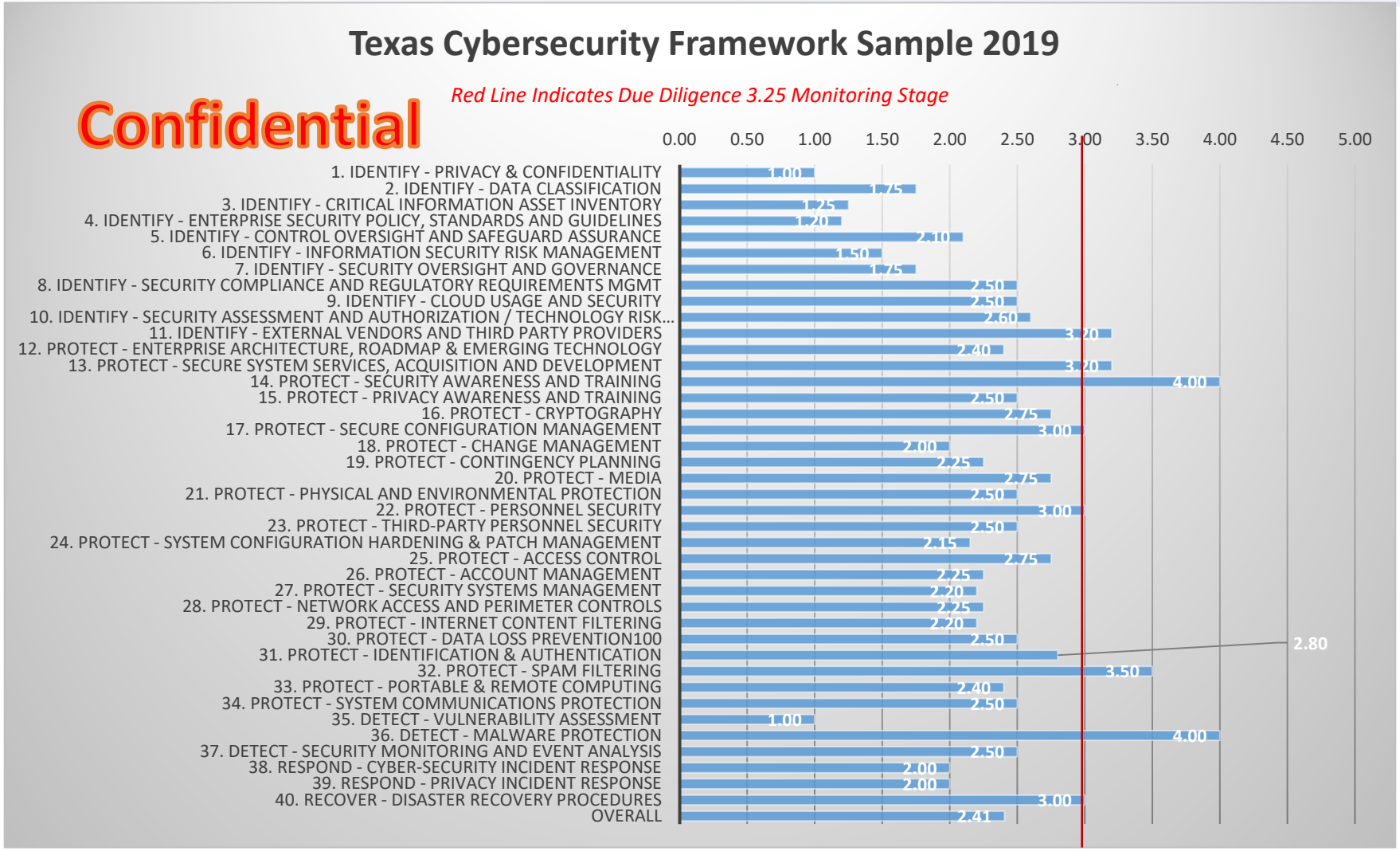
SB 820 Enforcement

Texas Cybersecurity Framework

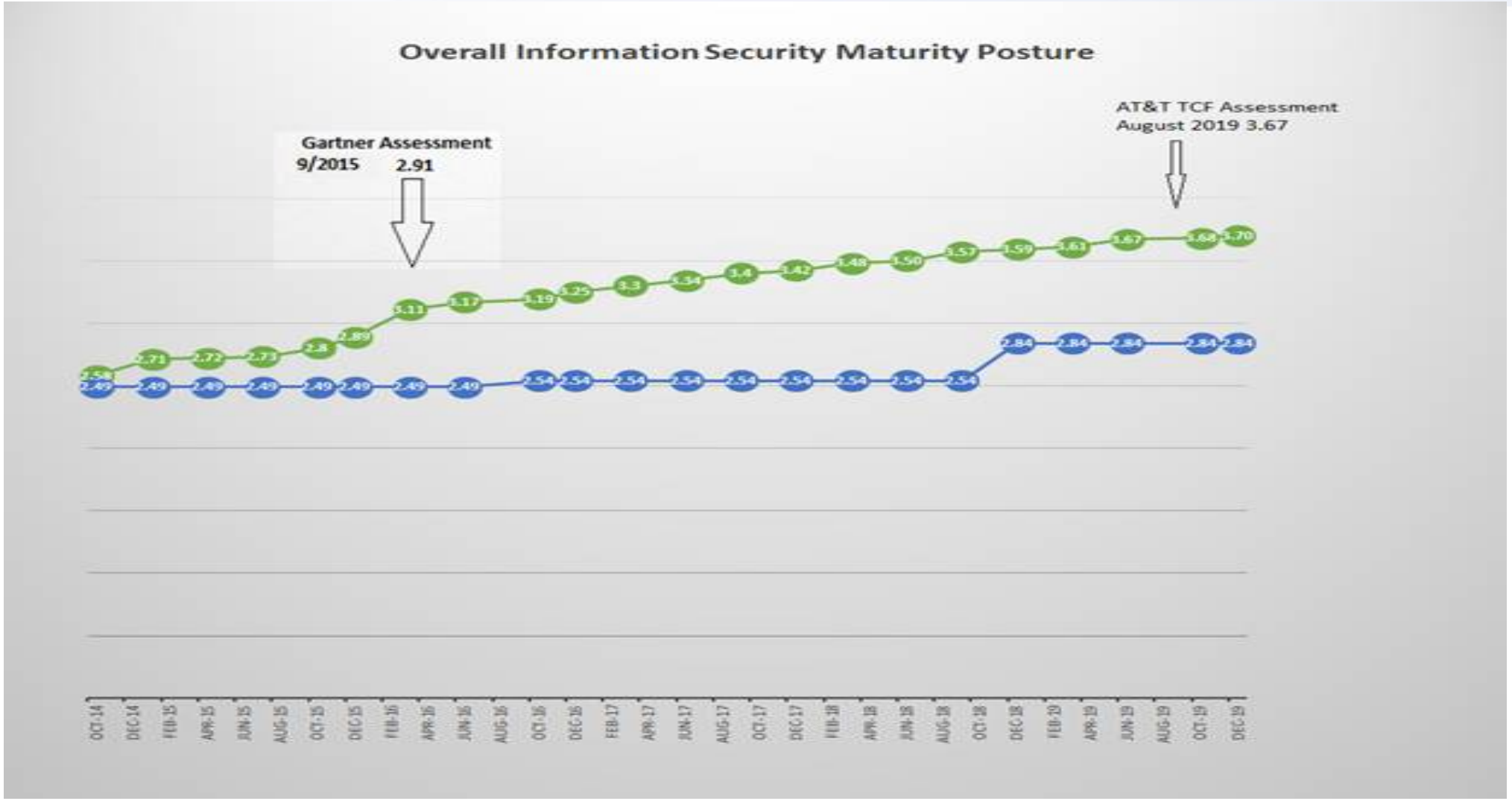
Five NIST Functions

- Identify
- Protect
- Detect
- Respond
- Recover

SB 820


Texas Cybersecurity Framework Sample 2019
Red Line Indicates Due Diligence 3.25 Monitoring Stage
Confidential
0.00 0.50 1.00 1.50 2.00 2.50 3.00 3.50 4.00 4.50 5.00
1. IDENTIFY - PRIVACY & CONFIDENTIALITY 1.00
2. IDENTIFY - DATA CLASSIFICATION 1.75
3. IDENTIFY - CRITICAL INFORMATION ASSET INVENTORY 1.25
4. IDENTIFY - ENTERPRISE SECURITY POLICY, STANDARDS AND GUIDELINES 1.20
5. IDENTIFY - CONTROL OVERSIGHT AND SAFEGUARD ASSURANCE 2.10
6. IDENTIFY - INFORMATION SECURITY RISK MANAGEMENT 1.50
7. IDENTIFY - SECURITY OVERSIGHT AND GOVERNANCE 1.75
8. IDENTIFY - SECURITY COMPLIANCE AND REGULATORY REQUIREMENTS MGMT 2.50
9. IDENTIFY - CLOUD USAGE AND SECURITY 2.50
10. IDENTIFY - SECURITY ASSESSMENT AND AUTHORIZATION / TECHNOLOGY RISK... 2.60
11. IDENTIFY - EXTERNAL VENDORS AND THIRD PARTY PROVIDERS 3.20
12. PROTECT - ENTERPRISE ARCHITECTURE, ROADMAP & EMERGING TECHNOLOGY 2.40
13. PROTECT - SECURE SYSTEM SERVICES, ACQUISITION AND DEVELOPMENT 3.20
14. PROTECT - SECURITY AWARENESS AND TRAINING 4.00
15. PROTECT - PRIVACY AWARENESS AND TRAINING 2.50
16. PROTECT - CRYPTOGRAPHY 2.75
17. PROTECT - SECURE CONFIGURATION MANAGEMENT 3.00
18. PROTECT - CHANGE MANAGEMENT 2.00
19. PROTECT - CONTINGENCY PLANNING 2.25
20. PROTECT - MEDIA 2.75
21. PROTECT - PHYSICAL AND ENVIRONMENTAL PROTECTION 2.50
22. PROTECT - PERSONNEL SECURITY 3.00
23. PROTECT - THIRD-PARTY PERSONNEL SECURITY 2.50
24. PROTECT - SYSTEM CONFIGURATION HARDENING & PATCH MANAGEMENT 2.15
25. PROTECT - ACCESS CONTROL 2.75
26. PROTECT - ACCOUNT MANAGEMENT 2.25
27. PROTECT - SECURITY SYSTEMS MANAGEMENT 2.20
28. PROTECT - NETWORK ACCESS AND PERIMETER CONTROLS 2.25
29. PROTECT - INTERNET CONTENT FILTERING 2.20
30. PROTECT - DATA LOSS PREVENTION100 2.50
31. PROTECT - IDENTIFICATION & AUTHENTICATION 2.80
32. PROTECT - SPAM FILTERING 3.50
33. PROTECT - PORTABLE & REMOTE COMPUTING 2.40
34. PROTECT - SYSTEM COMMUNICATIONS PROTECTION 2.50
35. DETECT - VULNERABILITY ASSESSMENT 1.00
36. DETECT - MALWARE PROTECTION 4.00
37. DETECT - SECURITY MONITORING AND EVENT ANALYSIS 2.50
38. RESPOND - CYBER-SECURITY INCIDENT RESPONSE 2.00
39. RESPOND - PRIVACY INCIDENT RESPONSE 2.00
40. RECOVER - DISASTER RECOVERY PROCEDURES 3.00
OVERALL 2.41

Overall Cybersecurity Maturity Posture



Quote for the Day

“Cybersecurity is not a weekend getaway, it is a journey.”

Frosty Walker

TEA CISO

Texas Cybersecurity Framework Roadmap

2.14	Protect	Security Awareness and Training	AT-01 AT-02 AT-03 AT-04	Define, prepare, deliver, and facilitate an ongoing awareness campaign utilizing a wide variety of mediums and delivery mechanisms to effectively and constantly educate the organization on security related information, threats, and technology risks.	1)Establish a Security Awareness Policy. 2)Define, prepare, deliver, and facilitate an ongoing Security Awareness campaign utilizing a wide variety of mediums and delivery mechanisms to effectively and constantly educate the organization on security related information, threats, and technology risks based on roles performed in the organization (i.e. privileged users (admins, DBA's), executive users, programmers, contractors and end users). 3)Role based training can consist of information as determined appropriate to perform job function from online training, instructor lead training or simple PowerPoint presentation. 4) Ensure that every employee, contractor, intern and affiliate is aware of the organization's approach and policies to protecting the assets and information within your organization. 5)The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance.

Texas Cybersecurity Framework Roadmap

#	FUNCTIONAL AREA	SECURITY OBJECTIVE	NIST FRAMEWORK MAPPING	DEFINITION/OBJECTIVE	Road Map Information (Recommendations to improve security posture)
2.1	Identify	Privacy & Confidentiality	AP-02 AR-01 AR-03 AR-07 AR-08 CA-03 DI-01 DI-02 DM-01 DM-02 DM-03 IP-01 IP-02 IP-03 SC-08 SI-07 SE-01 TR-01 TR-02 TR-03 UL-01 UL-02	Ensuring the appropriate security of retained information and approved sharing under defined conditions with required safeguards and assurance. Includes the requirements of HIPAA, Texas Business & Commerce Code, and agency defined privacy policies that include and expand upon regulatory and legal requirements for establishing contractual/legal agreements for appropriate and exchange and protection.	1)Ensuring the appropriate security of retained information and approved sharing under defined conditions with required safeguards and assurance. 2)Check for appropriate Identity Access Mgmt. (IAM) i.e. Onboarding & Off boarding processes, Principle of Least Privilege Access. 3)Establish and adhere to data retention policy. 4)Adherence to data protection requirements of FERPA, Texas Business & Commerce Code, Texas Education Code and entity defined privacy policies. 5)The organization should have a documented, detailed approach to meeting the objective, and regularly measures its compliance. 6)The organization should evaluate risk and integrate improvements beyond the requirements of applicable regulations on a regular basis.

Frameworks which can be considered for SB820

- NIST Cybersecurity Framework
- CIS RAM (Center for Internet Security Method)
- CIS CAT Lite (Center for Internet Security® Configuration Assessment Tool

https://www.cisecurity.org/blog/introducing-cis-cat-lite/

Frameworks which can be considered for SB820

EDUCATION (K - 12)

Our commitment to education is unmatched. There is no more virtuous cause that ensuring that our future leaders are able to learn in a secure environment while providing affordable access to leading cybersecurity capabilities.

Small & Medium Business

Understanding the need for Value is at the core of all business, but it is the heart beat of Small and Medium Businesses. We have opened a once unaccessible capability and priced it to win your business.

Enterprise & Higher Education

Ongoing visibility, effectively communicate, reduced risk and developing roadmaps remains elusive and costly for most enterprises. Leveraging technology, and our community of peers, we have unlocked one of cybersecurity's most challenging questions.

V3 CYBERSECURITY

Minerva

https://v3cybersecurity.com/

Ransomware

** source:* https://www.google.com/maps/d/viewer?mid=1UE6Nko9iRG1tLci_AeqgsxzxGzs&ll=40.75531828029828%2C-112.875968792219966&z=4

Ransomware Impact on Texas

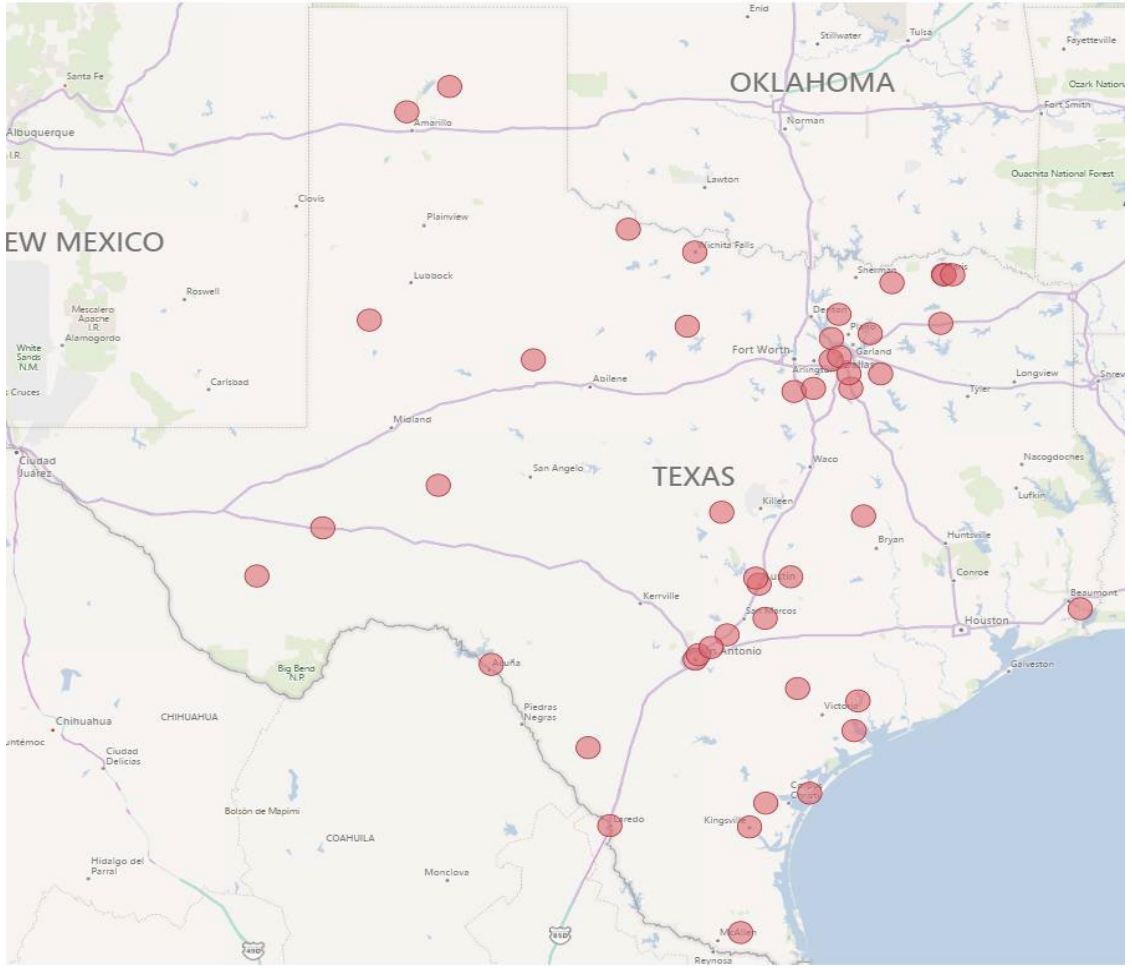
Senate Bill 64 (2019)

- A cybersecurity event is included in the definition of a disaster.
- Under Governor's orders, The National Guard may assist with defending the state's cyber operations.

14 - Texas School Districts reported an issue with Ransomware in 2019

321 - Average FTE hours spent to resolve issue

2019 Ransomware Impact on State and Local Governments



SOURCE: reported to DIR

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

Do’s and Don’ts

Do's 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!**

Thought for the day

“You can outsource everything, except responsibility.”

John Keel, Texas State Auditor

Questions?

Texas Education Agency

Thank you!