# Cybersecurity Tips and Tools – Cybersecurity Insurance, Is it Really a Good Investment for My School?

Frosty Walker

Chief Information Security Officer

Texas Education Agency

Frosty.Walker@tea.texas.gov

(512) 463-5095

# 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

# Texas Gateway - Cybersecurity Tips and Tools

# Are Cybersecurity Events a Real Threat?

**Senate Bill 64 (2019)**

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

# Nationwide K-12 Cyber Events since January 2016



Source: https://k12cybersecure.com/k12incidentmap
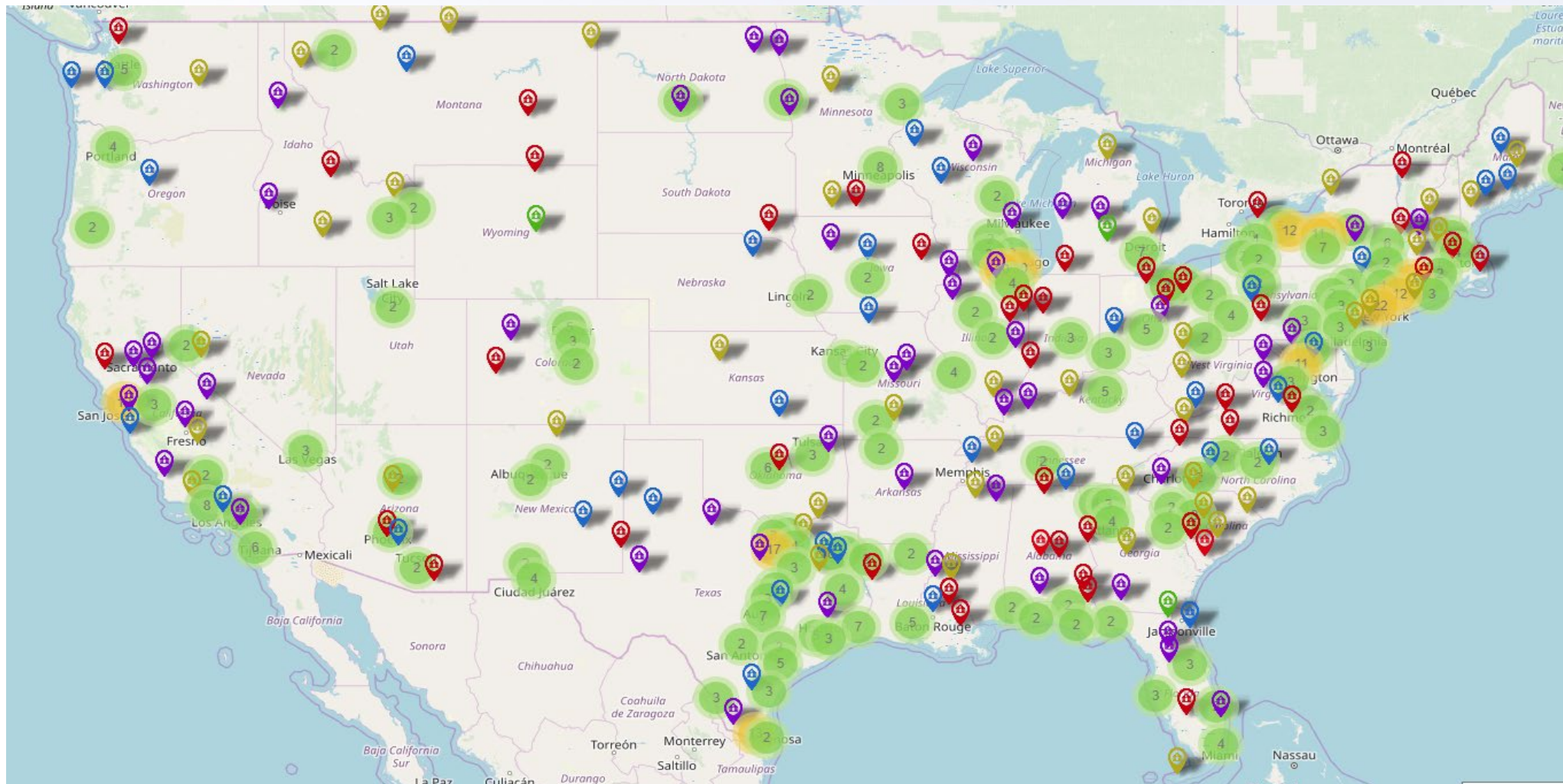
# Breakdown 2019 Texas Ransomware Incidents

| Organization Type | Number of Incidents |
|---|---|
| Cities | 23 |
| Counties | 9 |
| School Districts | 11 |
| Other Local Entities | 4 |
| State Agencies and Universities | 3 |

Source: Reported to DIR

# 2019 Texas Ransomware Incidents
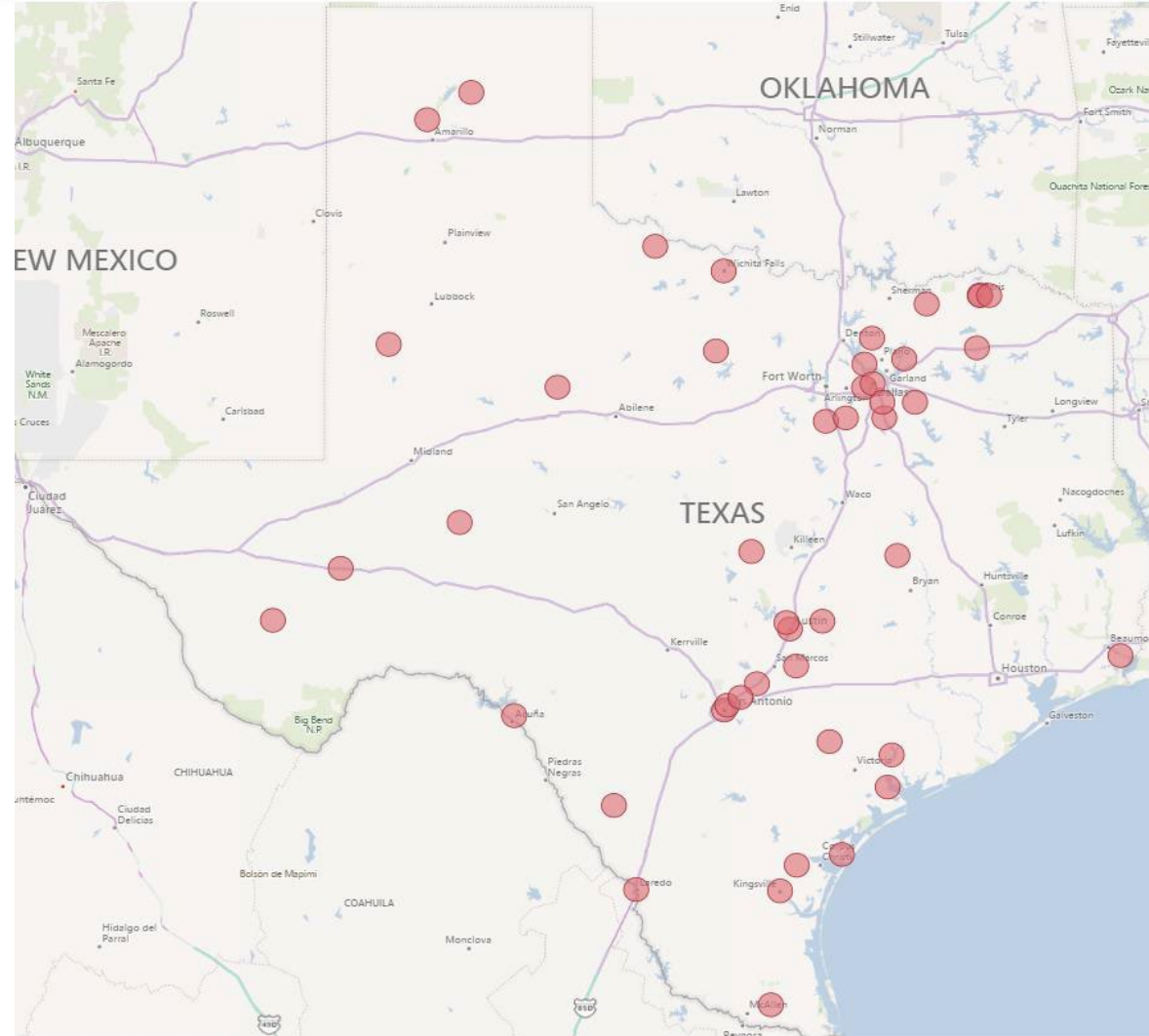
# By the Numbers

**Average cost per record exposed in a data breach in the United States**

**$242.00**

**Average size of data breach in the United States**

**25,575**

**Average cost of a data breach in the United States**

**$6,189,150**

**Source: Ponemon Institute *Cybersecurity Research Report***

# Case Study - Boulder Valley School District

- **August 2017 – fraudulent instruction**

- **$576M bond approved for campus renovation**

- **Accounts payable received a call from a 'representative' of the construction company**

- **Requested multiple account changes**

- **$850,000 sent to a bogus account**

- **April 2019 – ransomware/unpatched servers**

- **Compromised systems used for state standardized testing. Lost access to district learning management system (Canvas)**
  - Rescheduled standardized tests

- **Third party security company contracted ($$)**

- **System outage for over a week**
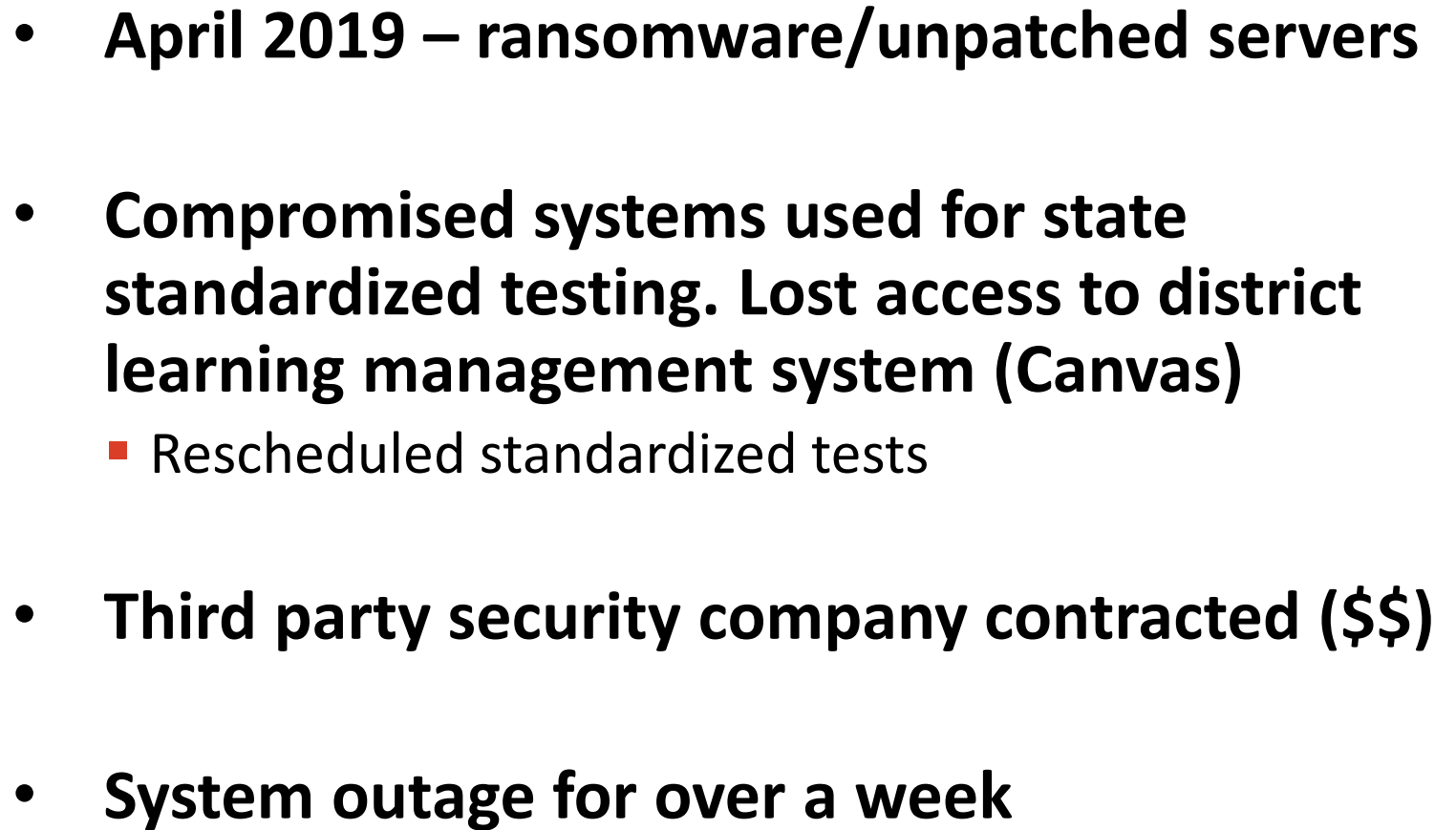
# Case Study - Scott County Schools, Kentucky

- **April 2019 – phishing Attack**

- **Outstanding invoice scam**

- **Paid the $3.7M invoice**

- **With FBI/bank assistance, the entire amount was recovered**

- **No claim filed**

1. ***It may be more affordable than you think.***

- Cyber liability insurance is still a fairly new concept, so there's a lot of variation among policies, and a lot of room for negotiation.

2. ***It can cover more than you think.***

- Some policies offer "first party" coverage--that is, they will pay you for things like business interruption, the cost of notifying customers of a breach, and even the expense of hiring a public relations firm to repair any damage done to your image as a result of a cyber attack.

## 3. You probably don't have a risk management team.

- An insurer might work with a small company to make sure a firewall is in place to protect your network, and make sure you have social media policies that reduce risk. Your insurer may well be willing to help with these areas because the better protected you are, the less likely you are to have a breach that could result in a claim.

## 4. Even if you don't host your data yourself, you're still responsible.

- "You can outsource anything, except responsibility"

    John Keel – former Texas State Auditor

**5.** *Your general policy won't cover you.*

- **Typically, a general liability policy specifically excludes losses incurred because of the Internet, so a good cyber liability policy can pick up where your general policy leaves off.**

# Cyber Liability Insurance Coverage

**Investigation:** A forensics investigation is necessary to determine what occurred, how to repair damage and how to prevent the same type of breach from occurring in the future. Investigations may involve the services of a third-party security firm, as well as coordination with law enforcement and the FBI.

**Business losses:** A cyber insurance policy may include similar items that are covered by an errors & omissions policy (errors due to negligence and other reasons), as well as monetary losses experienced by network downtime, business interruption, data loss recovery and costs involved in managing a crisis, which may involve repairing reputation damage.

# Cyber Liability Insurance Coverage

**Privacy and notification:** This includes required data breach notifications to customers and other affected parties, which are mandated by law in many jurisdictions, and credit monitoring for customers whose information was or may have been breached.

**Lawsuits and extortion**: This includes legal expenses associated with the release of confidential information and intellectual property, legal settlements and regulatory fines. This may also include the costs of cyber extortion, such as from ransomware.

# Keep in Mind that Cyber Insurance is Still Evolving.

Cyber risks change frequently, and organizations tend not to report the full impact of breaches in order to avoid negative publicity and damage the trust of customers. Thus, underwriters have limited data on which to determine the financial impact of attacks. Essentially, the true risk of cyberattacks is not completely understood.

# Cybersecurity Insurance Overview

**528 cyber insurers in 2018**

- Increase from 417 in 2017
- Top 10 writers held 69.5% of market
  - (Chubb, AXA US, AIG, Travelers, Beazley)

**Premiums (both standalone and packaged) increased 12% in 2018**

- $1.8 Billion to $2.0 Billion
- Double the number from 2015
- Slight slowdown from a 30% growth rate in previous two years

# Cybersecurity Insurance Overview

**Growth in cyber coverage driven by threat awareness and separation of coverage**

- 2018 55% was packaged
- 2017 45% was packaged

**Claims grew 37% in 2018**

- More than 12 million first party claims in 2018
  - Breach notifications
  - Credit Monitoring
  - Business Interruptions
- More small and medium sized organizations gaining coverage

# Cybersecurity Insurance Overview

**Considerations:**

**Right sizing coverage levels**
- Coverage is trending up as ransomware demands increase

**Understanding your policy**
- Business interruption?
- Fraudulent Instruction limitations
- Equipment?
- How many years of identity theft monitoring?

**Requirements?**
- Preferred Vendors

# Trends in Cybersecurity Claims

**2014-2020**

- **6 External Hacks**

- **7 Fraudulent Instruction**

- **20 Phishing Email Attacks**

- **15 Ransomware Attacks**

- **4 Stolen Technology/Device**

- **9 Unsecured Electronic Records**

- **3 Unsecured Physical Records**

# TASB Coverage

- **Privacy Liability (third party coverage)**

- **Response Services (first party coverage)**

- **Notifications**

# TASB Coverage

- **Ransomware**
- **Fraudulent Instruction**
- **Regulatory Proceeding**
- **Unauthorized Access or Use of Computer Systems**
- **Unauthorized Disclosure of Data (phishing, spoofed emails)**
- **External Hack (virus)**
- **Stolen or Lost Technology Device**
- **Access to Unsecured Electronic or Physical Records**

# TASB – Coverage Process

**In the event of a suspected Data or Security breach report incident as soon as possible!**

- If incident requires immediate attention, call: Marcy Barker, Liability Claims Manager, 855.295.8344

- You may also e-mail notice to Marcy Barker: marcelina.barker@tasb.org

# TASB - Coverage Process
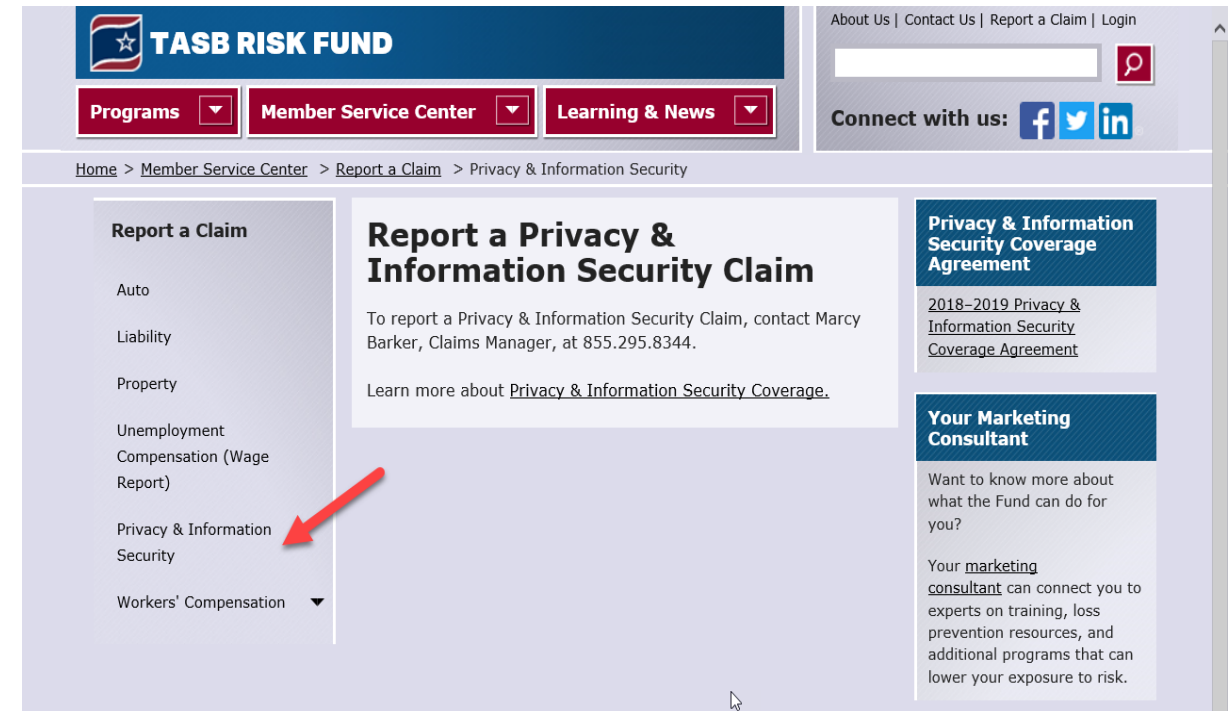
If services are to be engaged, the BBR team will schedule a follow-up call with the member, Fund rep. (Marcy) and recommended vendors.

Engagement Letters and Statements of Work will be executed by Marcy Barker on behalf of the member

If forensic experts are to be engaged, privacy counsel will direct the activity under an attorney-client privilege

Services incurred within coverage will be billed and paid by the Fund.

If the member is required to provide notice of the breach, privacy counsel will assist with the notifications and activation of credit monitoring.

Notifications are capped (refer to CCS)

Costs associated with notifications and credit monitoring will be billed and paid by the Fund up to the coverage limits

# Lessons Learned

**David Truman – Cuero ISD**

# Questions?

**Thank you!**