



# CYBER SECURITY TIPS AND TOOLS

## CYBERSECURITY/PRIVACY AWARENESS

Frosty Walker

Chief Information Security Officer

Texas Education Agency

[Frosty.Walker@tea.texas.gov](mailto: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, ESC's, TEA and the private sector.

# Texas Gateway

<https://www.texasgateway.org/>

## Cyber Security Tips and Tools

Three white diagonal lines of varying lengths and thicknesses are positioned in the bottom right corner of the slide, pointing towards the top right.

## Online resources FOR YOUR CLASSROOM

Find engaging, TEKS-aligned resources that you can use with your students as part of classroom instruction, intervention, acceleration, or additional practice.

show me more

BROWSE TEKS

BROWSE RESOURCES ▶

Search

### Featured Resources

Getting Started Guide

Starting the Conversation

ELA & READING  
Targeting the 2 Percent

Restorative Discipline Practices in Texas

SOCIAL STUDIES  
Social Studies TEKS: Supporting Information

MATH  
Teacher2Teacher Math Video Series

Teacher2Teacher

cyber security data  
Cyber Security Tips and Tools

Introduction to the Revised Mathematics TEKS  
MATH  
Mathematics TEKS: Supporting Information

ELA & READING  
OnTRACK English II Reading: Understanding and Analysis of Literary Text

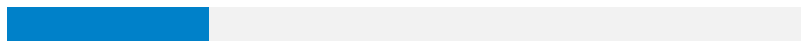




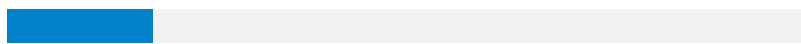
## Who's behind the breaches?

**75%** 

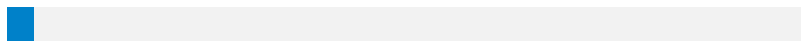
perpetrated by outsiders.

**25%** 

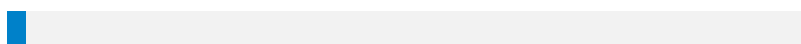
involved internal actors.

**18%** 

conducted by state-affiliated actors.

**3%** 

featured multiple parties.

**2%** 

involved partners.

**51%** 

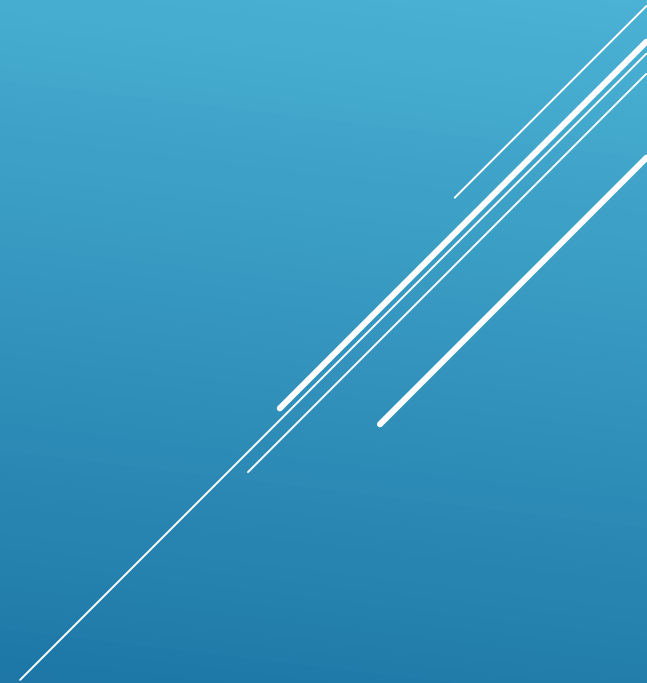
involved organized criminal groups.

**SOURCE: Verizon 2017 DBIR**

**In the Public sector – For the 2017 report, 40% of the data breaches (96 of 239 total) involved internal actors.**


SOURCE: Verizon 2017 DBIR

Why would schools be a target?



"If bad actors can access student [personal data], that information can be exploited for the purpose of fraud and committing crimes for years before it is detected."

Mary Kavaney, the chief operating officer of the Global Cyber Alliance

A decorative graphic consisting of several parallel white lines of varying lengths, slanted upwards from left to right, located in the bottom right corner of the slide.



## **Students:**

**FERPA (20 U.S.C. 1232g; 34 C.F.R. 99.3) defines “personally identifiable information” to include the student’s name, the name of the student’s parent or other family members, the address of the student or student’s family, a personal identifier (SSN, student number, biometric record), other indirect identifiers (DOB, place of birth, mother’s maiden name), or other information that alone or in combination is linked or linkable to a specific student that would allow a reasonable person in the school community to identify the student with reasonable certainty.**

**FERPA is applicable to personally identifiable information contained in education records. “Education records” means those records, files, documents, and other materials that contain information directly related to a student and are maintained by an educational agency or institution.**

## Students Continued:

FERPA and section 26.013 of the Texas Education Code address “directory information.” A school district is permitted to designate certain information about students as directory information that is publicly available. **However, a parent or eligible student must be given the opportunity to opt out of directory information. Directory information may include the student’s name, address, telephone number, email address, photograph, date and place of birth, grade level, enrollment status, dates of attendance, participation in recognized activities and sports, and honors and awards received.**

Section 39.030 provides the results of **individual student performance on academic skills assessment instruments are confidential and may be released only in accordance with FERPA.** However, overall student performance data must be aggregated by ethnicity, sex, grade, subject, campus, and district and made available to the public. This data may not contain the names of individual students or teachers.

## **Educators/District Employees:**

Section 21.0481 of the Education Code provides **the results (numerical score and pass/fail) of educator certification examinations are confidential.**

Section 21.355 of the Education Code states a **document evaluating the performance of a teacher or administrator is confidential.**

Section 22.08391 of the Education Code provides **criminal history record information must not be disclosed except under certain circumstances.**

Section 552.117 of the Government Code **provides the home address and phone number, emergency contact information, social security number, or information that reveals whether the individual has family members is excluded from public disclosure if the current or former employee of a government body makes the election to withhold such information** under section 552.024 of the Government Code.

## **Educators/District Employees continued:**

Section 552.126 of the Government Code provides **the name of an applicant for the position of superintendent of a school district is excluded from public disclosure, except the board of trustees must give public notice of the name(s) of the finalists being considered at least 21 days before the date of the meeting at which final action or vote is to be taken on the employment of the person.**

Section 552.135 of the Government Code provides **an informer's name or information that would substantially reveal the identity of an informer is excluded from public disclosure. "Informer" is defined as a student or former student or an employee or former employee of a school district who has furnished a report of another person's or persons' possible violation of criminal, civil, or regulatory law to the school district or the proper regulatory enforcement authority.**

Section 552.136 of the Government Code provides **a credit card, debit card, or access device number (a card, code, account number, etc. used to obtain money, goods, or services) is confidential.**

## Information regarding Cybersecurity Posture

Sec. 552.139. EXCEPTION: CONFIDENTIALITY OF GOVERNMENT INFORMATION RELATED TO SECURITY OR INFRASTRUCTURE ISSUES FOR COMPUTERS. (a) Information is excepted from the requirements of Section 552.021 if it is **information that relates to computer network security**, to **restricted information** under Section 2059.055, or to the **design, operation, or defense of a computer network**.

(b) **The following information is confidential:**

(1) a **computer network vulnerability report**;

(2) any other **assessment of the extent to which data processing operations, a computer, a computer program, network, system, or system interface, or software of a governmental body or of a contractor of a governmental body is vulnerable to unauthorized access or harm**, including an assessment of the extent to which the governmental body's or contractor's electronically stored information containing sensitive or critical **information is vulnerable to alteration, damage, erasure, or inappropriate use**;

## Texas Protective Requirements

Texas Business Code

Sec. 521.052. BUSINESS DUTY TO PROTECT SENSITIVE PERSONAL INFORMATION. (a) A business shall **implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure any sensitive personal information collected or maintained** by the business in the regular course of business.



## Breach Notification Requirements

Texas Business Code

Sec. 521.053. NOTIFICATION REQUIRED FOLLOWING BREACH OF SECURITY OF COMPUTERIZED DATA. (a) In this section, "**breach of system security**" means **unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information** maintained by a person, **including data that is encrypted if the person accessing the data has the key required to decrypt the data**. Good faith acquisition of sensitive personal information by an employee or agent of the person for the purposes of the person is not a breach of system security unless the person uses or discloses the sensitive personal information in an unauthorized manner. (b) A person who conducts **business in this state and owns or licenses computerized data that includes sensitive personal information shall disclose any breach of system security, after discovering or receiving notification of the breach, to any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person**. The disclosure shall be made as quickly as possible, except as provided by Subsection (d) or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

“You can outsource everything, except responsibility.”

John Keel, Texas State Auditor

A decorative graphic consisting of several parallel white lines of varying lengths, slanted upwards from left to right, located in the bottom right corner of the slide.




**2017 U.S. cost per record breached, per research conducted by the Ponemon Institute.**

**\$265.00**

\*Direct expenses include engaging forensic experts, outsourcing hotline support and providing free credit monitoring subscriptions and discounts for future products and services. Indirect costs include in-house investigations and communication, as well as the extrapolated value of customer loss resulting from turnover or diminished customer acquisition rates.

## What should be included in a successful Cybersecurity Awareness Training program?

- Social Engineering
  - Email, Phishing, & Messaging
  - Browsing
  - Social Networks
  - Mobile Device Security
  - Passwords
  - Encryption
  - Data Security and Data Destruction
  - Insider Threats
- 

## What should be included in a successful Privacy Awareness Training program?


- Family Educational Rights and Privacy Act (FERPA)
  - Privacy
  - Data Security and Data Destruction
- 

## **Who should receive the Cybersecurity/Privacy Awareness Training?**


**Everyone who may have access to Sensitive Information**

- Administration
  - Staff
  - Contractors
  - Interns
  - Vendors
  - Students
- 
- A decorative graphic consisting of several parallel white lines of varying lengths, slanted upwards from left to right, located in the bottom right corner of the slide.

## **When should they have Cybersecurity/Privacy Awareness Training?**

- New employee orientation briefing
  - Online training completed within 30 days from start date
  - Annually thereafter
- 

## **Components of a successful Cybersecurity/Privacy Awareness Program**

- New Employee Orientation Briefing
  - Computer based training
  - Instructor lead training
- 

## **Security Awareness Vendors:**

Secure the Human

Knowbe4

Wombat

Free Cybersecurity Training

<https://www.cybrary.it>

Teacher Training Center

[https://edutrainingcenter.withgoogle.com/digital\\_citizenship/preview](https://edutrainingcenter.withgoogle.com/digital_citizenship/preview)

Elementary Student Training

<https://beinternetawesome.withgoogle.com/>

Questions?

