



# CYBERSECURITY TIPS AND TOOLS- PRACTICE, PRACTICE, PRACTICE

Frosty Walker

Chief Information Security Officer

Texas Education Agency

[Frosty.Walker@tea.texas.gov](mailto:Frosty.Walker@tea.texas.gov)

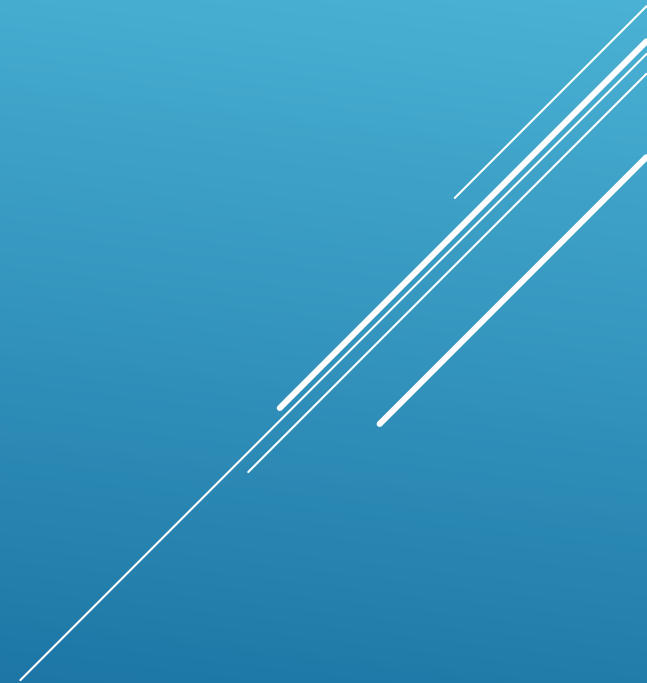
(512) 463-5095



# 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, ESCs, TEA and the private sector.



# Texas Gateway

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

## Cybersecurity Tips and Tools

Three parallel white lines of varying lengths and positions, slanted diagonally from the bottom right towards the top right, serving as a decorative element.



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

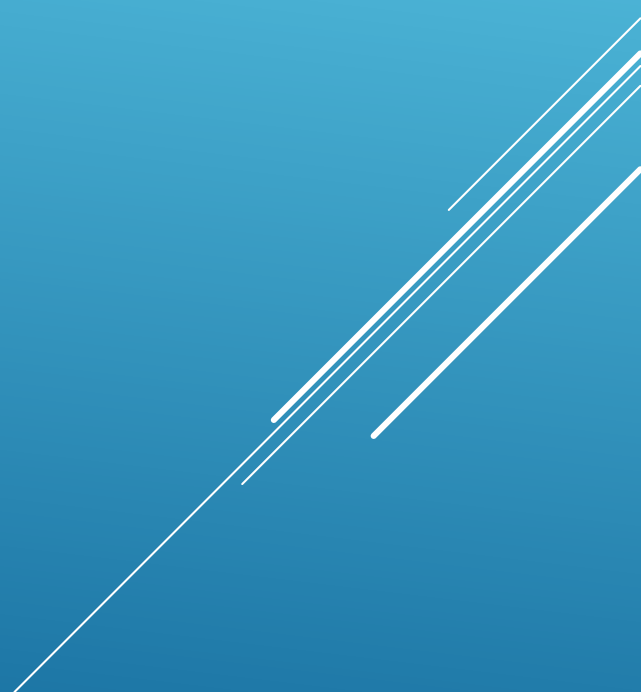
Search

Featured Resources

1 of 2

 <p>EARLY CHILDHOOD Prekindergarten Enrollment Toolkit</p>	 <p>MATH ESTAR/MSTAR</p>	 <p>Open-Source Instructional Materials</p>	 <p>openstax STUDY EDGE</p>	 <p>Cybersecurity Tips and Tools</p>	 <p>Restorative Discipline Practices in Texas</p>
 <p>ELA &amp; READING Complete "Red Book Series" Focused on Reading Instruction</p>	 <p>TEXAS LESSON STUDY Texas Lesson Study Briefing</p>	 <p>Starting the Conversation</p>	 <p>MATH TEA Statistics</p>	 <p>Statistics</p>	

# Building an incident response exercise



# Practice, Practice, Practice

## Choose an application for the Exercise


- **Public Facing**
- **Potentially contains sensitive information**

## **Choose a Method of Compromise**

- **Compromised Credentials**
  - **Application Vulnerability**
- 
- 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.



## Today's Exercise

- **Publicly facing application with sensitive information**
  - **Compromised credentials**
  - **International logins at unusual times**
- 
- 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.



# **Exercise, Exercise, Exercise!!!!**

- **Alert Notification**
- **Application team detects high volume of traffic during non-peak hours of operation with 100's of successful logins and notifies ISO**

**Exercise, Exercise, Exercise!!!!**

**Activate Incident Response Plan**


**Engage your Incident Response team**

**(Incident Response Team Redbook)**

A decorative graphic consisting of several parallel white lines of varying lengths, slanted diagonally from the bottom right towards the top right, located in the lower right quadrant of the slide.

**Exercise, Exercise, Exercise!!!!**

**Check with some of the users to verify if they logged in from international IP's during unusual hours.**

A decorative graphic consisting of several parallel white lines of varying lengths, slanted diagonally from the bottom right towards the top right, located in the lower right quadrant of the slide.


**Exercise, Exercise, Exercise!!!!**

**Disable USERID's or take the application out of service.**

Decorative white lines consisting of several parallel diagonal strokes in the bottom right corner of the slide.

**EXERCISE, EXERCISE, EXERCISE!!!!**

**Leadership decision—Is your application safe to continue operation, or do you need to suspend availability?**

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.

**EXERCISE, EXERCISE, EXERCISE!!!!**

**Application not available notifications**

**External communication**

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.

**EXERCISE, EXERCISE, EXERCISE!!!!**


**Continue investigation**

**Involve Application team to determine if the application logs can provide information as to what the 100 USERID's accessed. This will narrow the scope of your potential expose.**



**EXERCISE, EXERCISE, EXERCISE!!!!**

**Communication to leadership based on  
scope of exposure or potential exposure of  
the complete data set**

A decorative graphic consisting of several parallel white lines of varying lengths, slanted diagonally from the bottom right towards the top right, set against a blue gradient background.

# **EXERCISE, EXERCISE, EXERCISE!!!!**

- **Draft of breach notification**
- **Decision on best notification method**

Texas Business and Commerce Code Ch. 521, §521.053

- **Will you provide credit monitoring?**
- **Draft media communication**

## EXERISE PLAYBOOK Day 1

### EXERCISE ONLY NO EXTERNAL COMMUNCATIONS WILL BE SENT

12:00pm Application team reports higher than normal volume of activity on **Application X** during off peak hours to security team.

***Can Application team determine this issue from the logs and do they review on a regular basis?***

12:15pm Security team opens Incident Response event and begins a deep dive.

***Potentially use Incident Response Redbook as a guideline***

12:30pm ISO notifies CIO of potential information security issue.

13:00pm Network team notifies ISO of high volume of activity - anomaly on firewall logs to IP address for **Application X** from offshore IP addresses from midnight to around 4:00am

13:15pm Incident Response team asks Network team for assistance in reviewing firewall logs for midnight to 4:00am for activity from offshore IP addresses to see if any other applications may be seeing similar patterns of behavior. **(2 FTE hours)**

***Standard procedure for firewall log review to look for offshore IP ranges that were Identified and any other anomalies.***

## EXERISE PLAYBOOK Day 1

### EXERCISE ONLY NO EXTERNAL COMMUNICATIONS WILL BE SENT

13:30pm Incident Response team asks Application team to verify if higher volume of activity maps with time frames identified by Network team. **(1 FTE hour)**

***Standard procedure to review application logs for authentications during off peak hours***

14:45pm Application team notifies security team of confirmation of over 100 users authenticated into ***Application X*** between midnight and 4:00am.

15:00pm Incident Response team is able to match up firewall logs with ***Application X*** logs to confirm ***Application X*** users logging in during normal off peak activity hours from offshore IP addresses.

**(4 FTE hours)**

***Do you have the ability to do this (synchronized time)?***

15:15pm Incident Response team contacts some of the end users that logged in to ***Application X*** during off peaks hours from offshore IP address and the users contacted indicated they were home asleep between midnight and 4:00am. **(2 FTE hours)**

***Is contact information for end users available?***

15:45pm ISO advises CIO of issue and recommends taking ***Application X*** off line until cause is determined.

16:00pm CIO 1\*1 meeting with executive leadership to advise of issues and discuss taking ***Application X*** and all effected applications offline. **(30 minute meeting)**

***End users will need to be notified of unscheduled outages via standard notification process.***

## EXERISE PLAYBOOK Day 2

### EXERCISE ONLY NO EXTERNAL COMMUNICATIONS WILL BE SENT

9:00am Incident Response team provides list of **Application X** UserID's that were authenticating between midnight and 4:00am to the Application team to see if we can determine what data these users accessed in **Application X** (potential unauthorized access of sensitive information) **(4 FTE hours)**

*Potential review of application logs to see if we can extract this information from application logs or if there may be other ways to determine what was accessed*

14:30pm Application team confirms UserID's listed did access sensitive information during off peak hours.

*Confirmation of unauthorized access of sensitive information!*

15:30pm CISO and CIO have 1\*1 meeting with executive leadership to confirm as many as 1000 sensitive records have been exposed to unauthorized access. **(30 minute meeting)**

## EXERISE PLAYBOOK Day 2

### EXERCISE ONLY NO EXTERNAL COMMUNICATIONS WILL BE SENT

16:00pm ISO provides a list of users who have been exposed to each of the data owners with an explanation of how they will be involved in the approval of the notification letter after it has been reviewed by your Legal Counsel. **(30 minute meeting)**

*IT will verify we have contact information for the list of exposed users from different applications.*

17:00pm Communications team asked to draft media release regarding unauthorized exposure of approximately 1,000 sensitive records exposed to unauthorized access and that the investigation is ongoing. **(4 FTE hours)**

17:15pm Notification to end users of **Application X** will be available tomorrow morning at 8:00am with forced change password.

*You may need to setup a special helpdesk to assist end users.*

17:30pm Exposure notification process begins and will take approximately 2 weeks. **(2 hours of meeting over 2 weeks)**

*Discussion whether to provide credit monitoring and include information in notification.*

# GAP ANALYSIS

- Can your Application/Network team detect high volumes of traffic after hours?
  - a) What would the cost be to add the capability?
- Can the Network/Security team analyze traffic to see if it is from an international IP address?
- Can your teams match up the timing of the logs?
- Do the application logs indicate what was accessed by the users?
- Will your leadership take an application out of service based on the findings?
- If you need to send breach notification, will you provide credit monitoring?



Questions?

