Governance Authority Committee

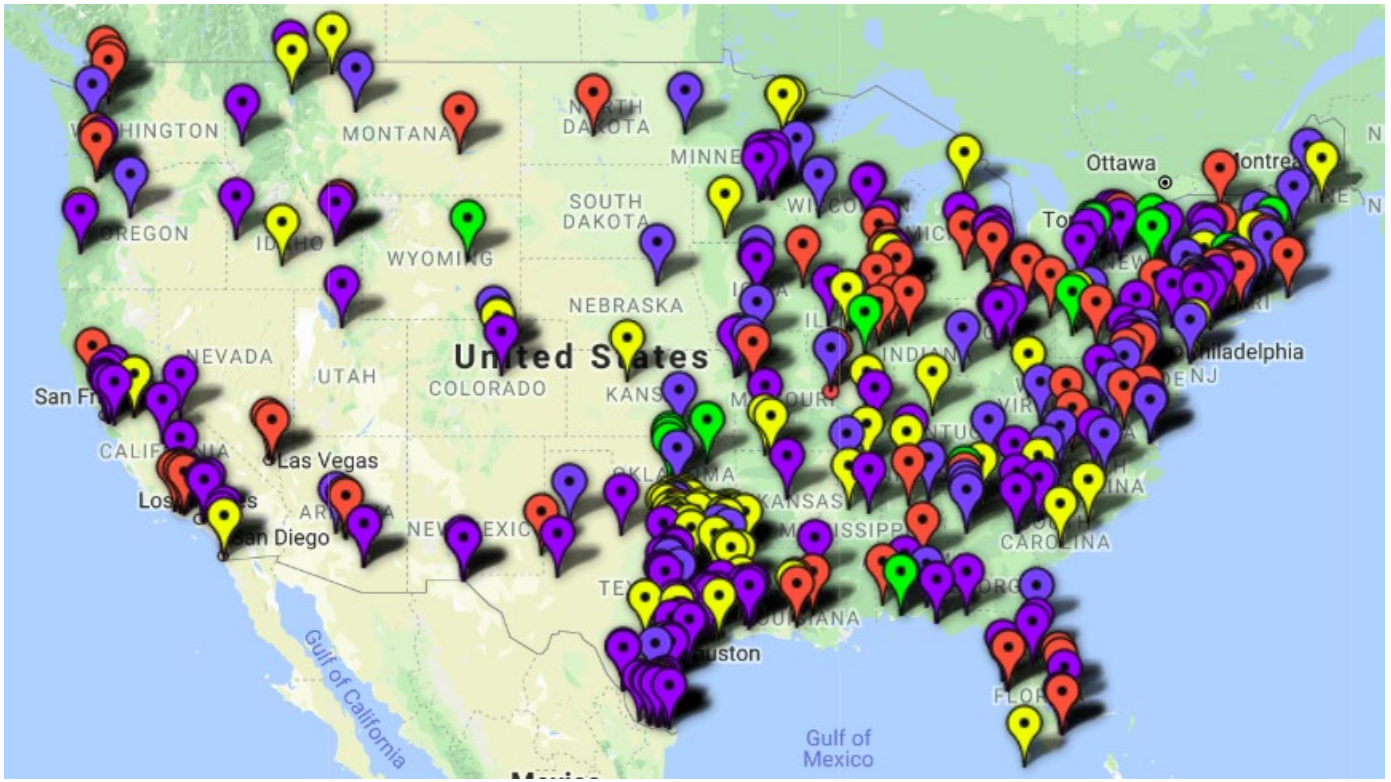
December 10, 2018

Today's Agenda

- **Current Events: Cyber Attacks in K12**
- **CFISD Committee Development**
- **Implemented Security Frameworks**
  - National Institutes of Science and Technology (NIST)
  - Trusted Learning Environment (TLE)
- **Recent Implementations**
  - LEARN Network (Lonestar Education and Research Network)
  - Resource Review
  - Data Privacy Agreement
- **Action Items Escalated from the Internet Advisory Committee**
  1. Modify verbiage in the Student Handbook should be modified to ensure clarity regarding student login processes.
  2. Require teachers to ensure the websites students are asked to review at home are accessible on the district network.
  3. Require employees complete the Cybersecurity training distributed by Technology Services.

K12 Cyber Attacks

- K12 Cyber Attacks - 391 incidents since January, 2016 across the US
- Florida Virtual Schools incident



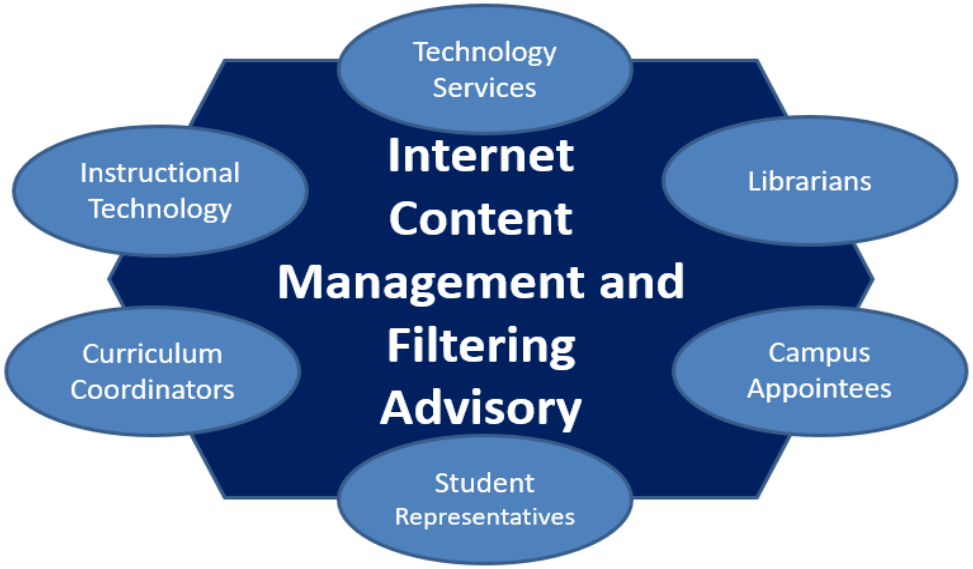
Area K12 Cyber Attacks

	District	Description
2016	Katy	Katy ISD warned about 78,000 of its students and staff members that their personal data - including social security numbers, names and birth dates - may have been accessed during a security breach
2016	North East	The district says that there were three separate ransomware incidents over the past two months. 20 campuses and two departments were affected. About 2.5 terabytes of data were encrypted, but no student personal information was compromised.
2016	Pearland	Pearland ISD refused to fork over about $1,600 in ransom demanded in two attacks this year, losing about three days of work from teachers and students. The district invested tens of thousands of dollars on security software.
2017	Kountze	A hacker accessed through an unsecured remote desktop used to access school computers from external locations. The hacker was able to lock the shared user files of all 1,300 students and employees. The district was able to restore their files.
2017	Splendora	Splendora ISD says a cyber-attack has compromised information of families within the district and could potentially give rise to threatening messages made directly to parents, students and staff.
2017	Spring Branch	A local high school student is accused of hacking a school's computer system and changing grades. The student faces a state jail felony charge.
2017	Multiple	The names and social security numbers of employees were made public on a website managed by the Texas Association of School Boards
2017	Multiple	Texas Dept of Agriculture employee's state-issued laptop computer was compromised through a malicious ransomware attack. The information included student names, social security numbers, home addresses, birthdates, and personal phone numbers of the affected students and their families.
2018	Rockdale	District officials said an employee responded to an email from a scammer pretending to be the superintendent. They requested copies of all the W2 forms for district employees. More than 350 employees had their personal information stolen.

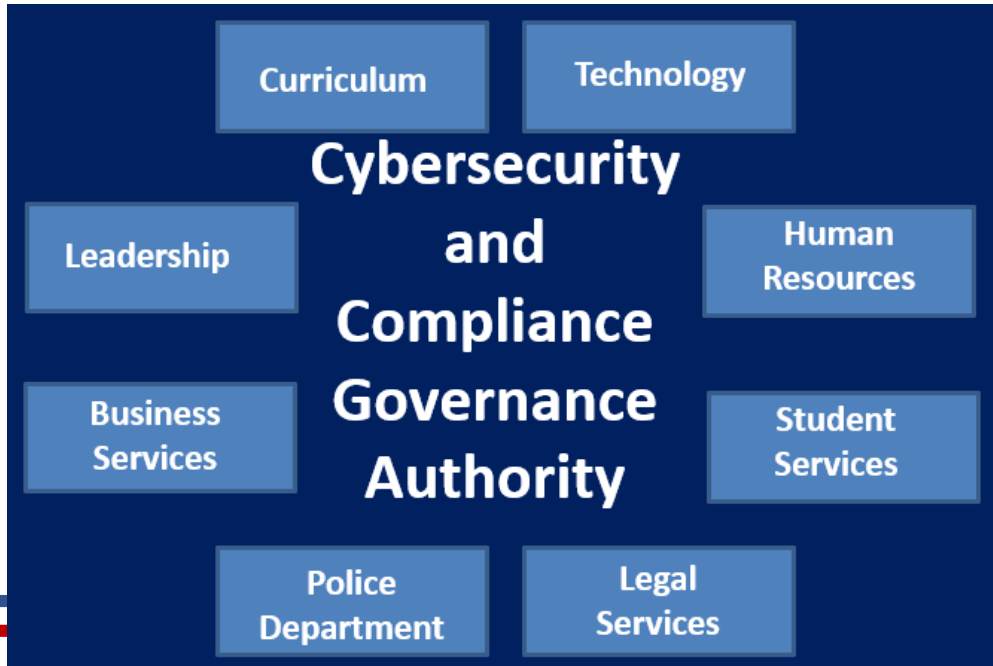
Unauthorized disclosure/breach
Ransomware
Phishing

Committee Development

- **Internet Advisory Committee**
  - **Purpose:** To **make recommendations, provide feedback, and disseminate information** as it relates to the protection, privacy, and security of students, employees, and personal data.



- **Governance Authority Committee**
  - **Purpose:** To **develop and implement** data privacy and security policies and practices as it relates to the protection, privacy, and security of students, employees, and personal data.



Internet Advisory Committee

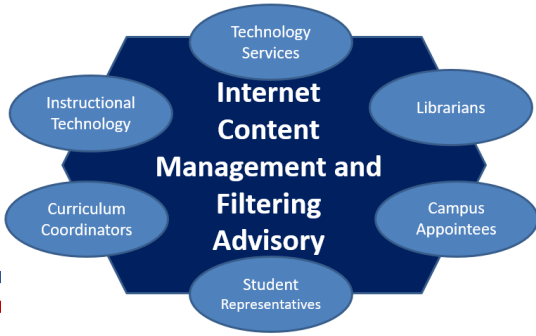
- **Purpose:** To **make recommendations, provide feedback, and disseminate information** as it relates to the protection, privacy, and security of students, employees, and personal data.

Curriculum
Diane Garland
Jenifer Jones
John Morrison
Kay Pechacek
Linda Sams
David Srubar
Stefanie Ware

Instructional Technology
Becky Cook
Todd Sepulveda
Steven Stone

Librarians
Jennifer Hill
Deborah Jones
Beth Keene
Mary Bridget Maddan
Heather McGuire
Andrea Morris
David Srubar
Stefanie Ware

Technology Services
Larry Barrios
James Costello
Becky Cook
John Crumbley
Frankie Jackson
Jennifer Miller
Eric Pina
Paula Ross
Greg Rhodes



Governance Authority Committee

- **Purpose:** To **develop and implement** data privacy and security policies and practices as it relates to the protection, privacy, and security of students, employees, and personal data.

Business & Financial Services
Mable Isles
Melissa McAnear
Karen Smith

Curriculum
Becky Cook
Lana Mock
Denise Kubecka
Barbara Levandoski
Kenya Turner

Human Resources
Jan Price
Jill Smith

Legal Services
Marney Sims

Principals
Heather Bergman
Cheryl Fisher
Sarah Harty
Cathryn Jacobs
Gary Kinninger
Maria Mamaux
Onica Mayers
Michelle Rice

Police Chief
Eric Mendez

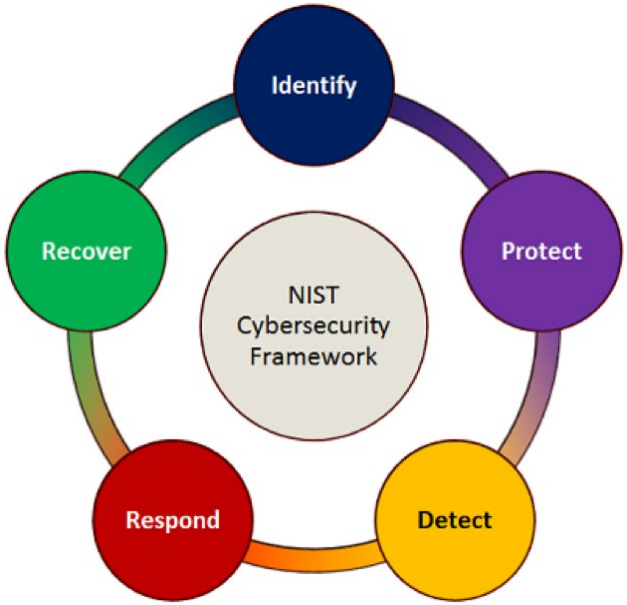
Student Services
Candy McCown
Jae Simpson-Butler

School Leadership & Administration
Sheri McCaig

Technology Services
Larry Barrios
James Costello
Frankie Jackson
Jennifer Miller
Eric Pina
Greg Rhodes
Paula Ross

Supporting Frameworks

- National Institutes of Standards and Technology (NIST)



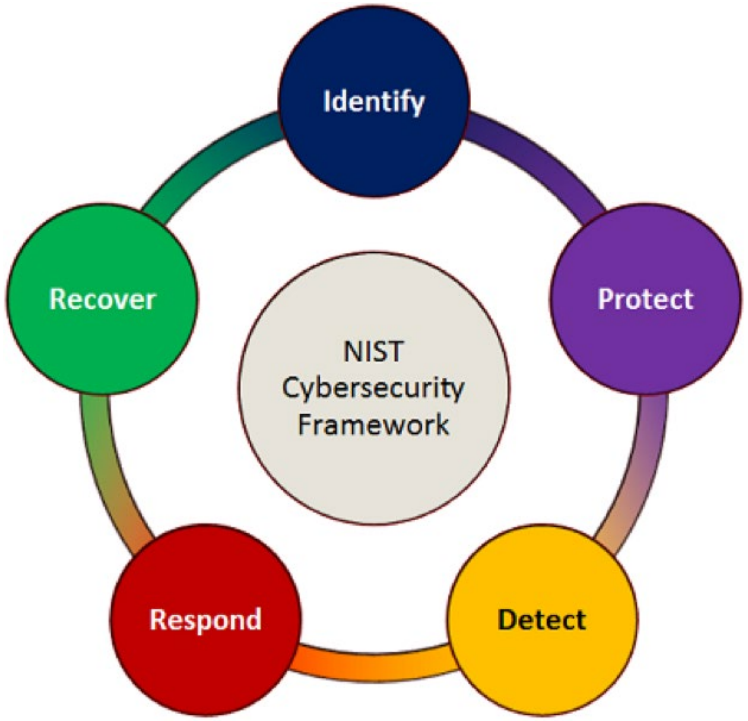
- Trusted Learning Environment (TLE)

TRUSTED LEARNING ENVIRONMENT

NIST Cybersecurity Framework

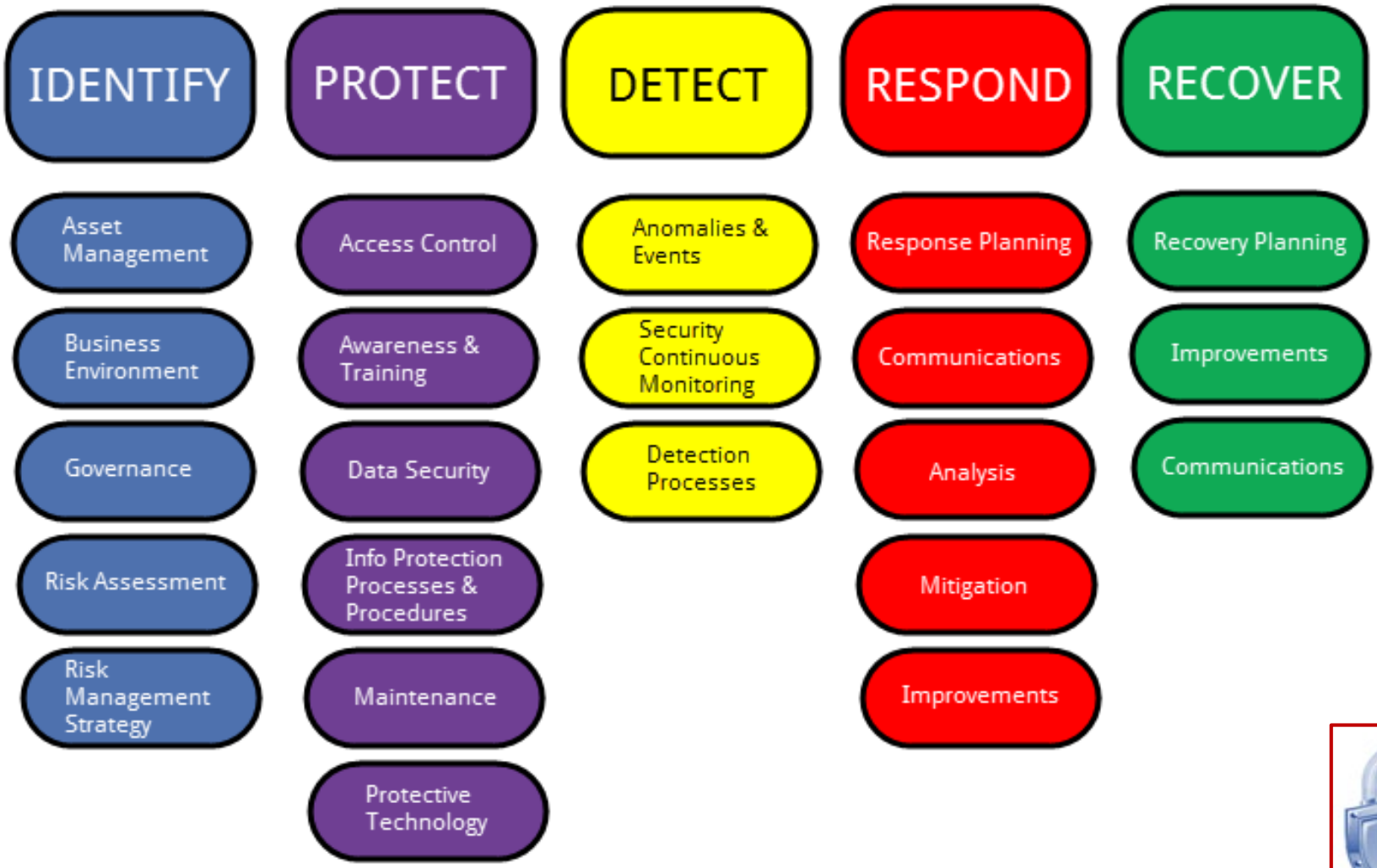
- Best practices created to prevent, detect, and respond to cyber-attacks.

- Goals of using a framework:
  - To improve the protection, privacy, and security of students, employees, and district data.
  - Align with regulations such as FERPA, CIPA, COPPA, and PPRA.

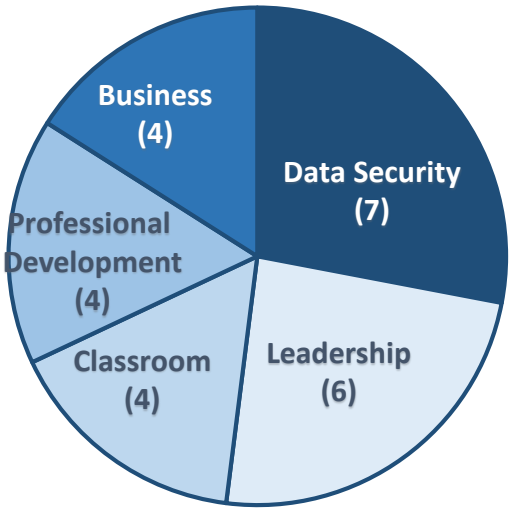


NIST Cybersecurity Framework

5 Functions, 22 Categories, and 98 subcategories



Trusted Learning Environment Framework



Practices in each category

- Leadership Practices
  - Manage and collaborate with stakeholders regarding the **use and governance of student data** to inform instruction
- Business Practices
  - Establish **acquisition vetting processes** and contracts that, at a minimum, address applicable compliance laws while supporting innovation.
- Data Security Practices
  - Perform **regular audits of data privacy and security practices** and publicly detail these measures
- Professional Development Practices
  - Require school staff to **conduct privacy and security training** and offer the instruction to all stakeholders
- Classroom Practices
  - Implement **educational procedures and processes** to ensure transparency while advancing curricular goals

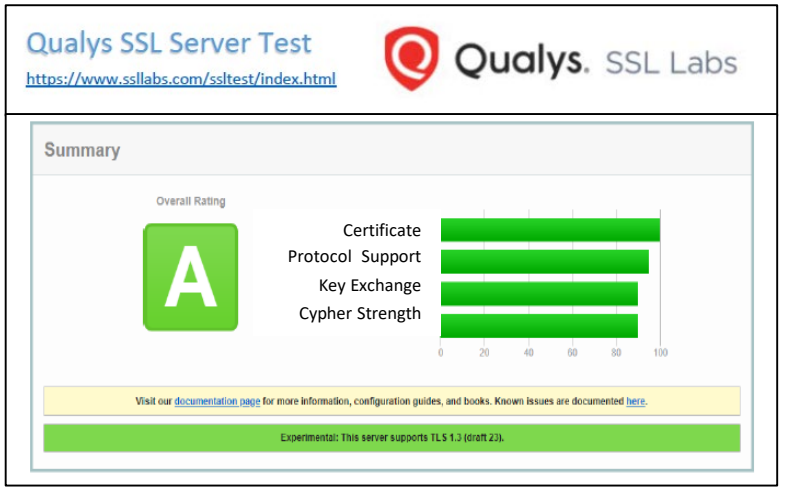
https://trustedlearning.org/framework/

Implemented Solutions

- LEARN Network

- Resource Review
  - Website
  - Software

- Data Privacy Agreement

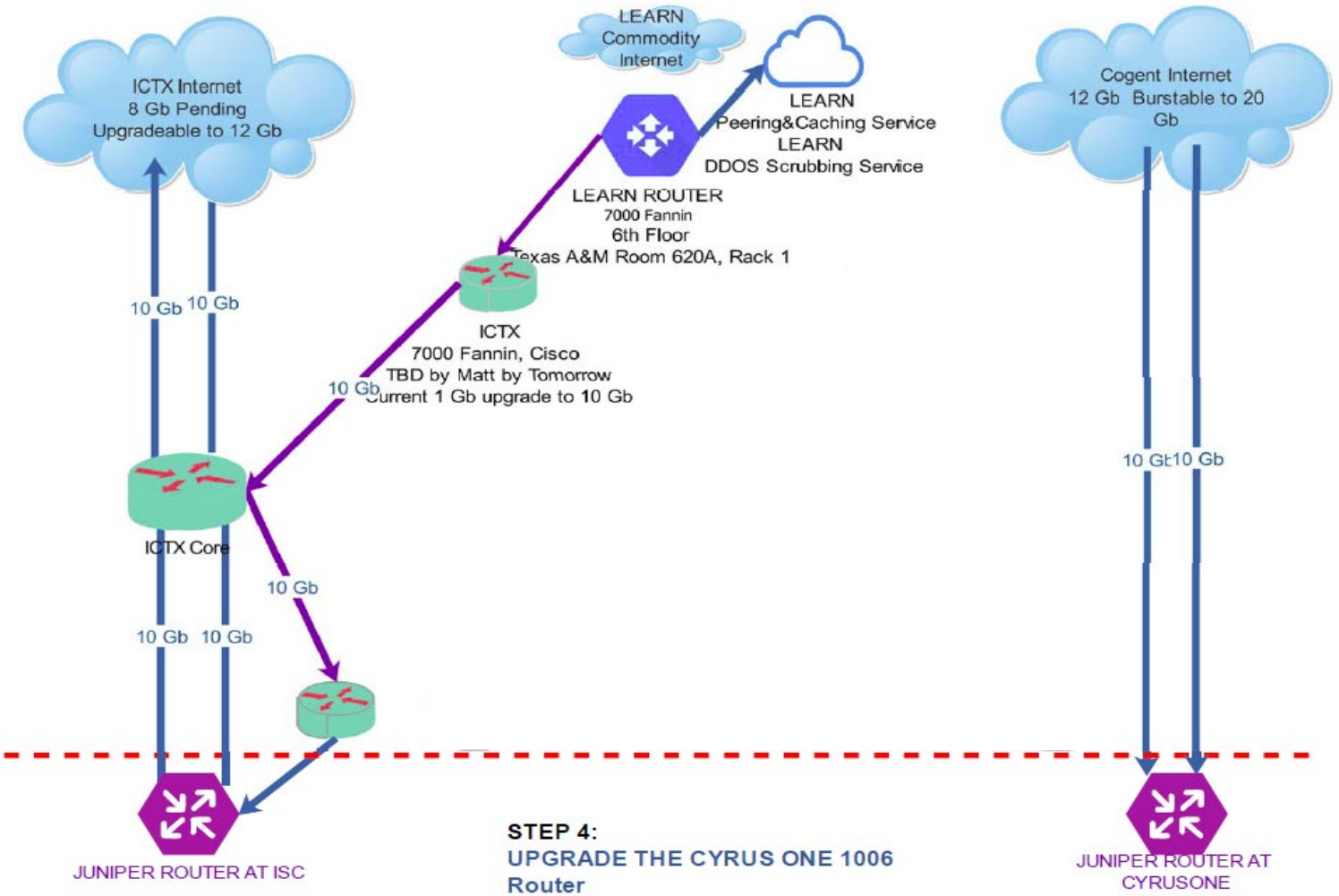


CFISD Resources

This database lists the vetted, approved, and declined resources that may be utilized by CFISD teachers and staff.

Status Key	**Approved:** Contract is signed and app is in use. **Approved w/ Guardian Release**: Guardians signed a contract to allow it to be used in a specific classroom with a specific group of students. **Not Approved:** Vendor was unable to sign the contract and, therefore, teachers are not allowed to use the app with students.

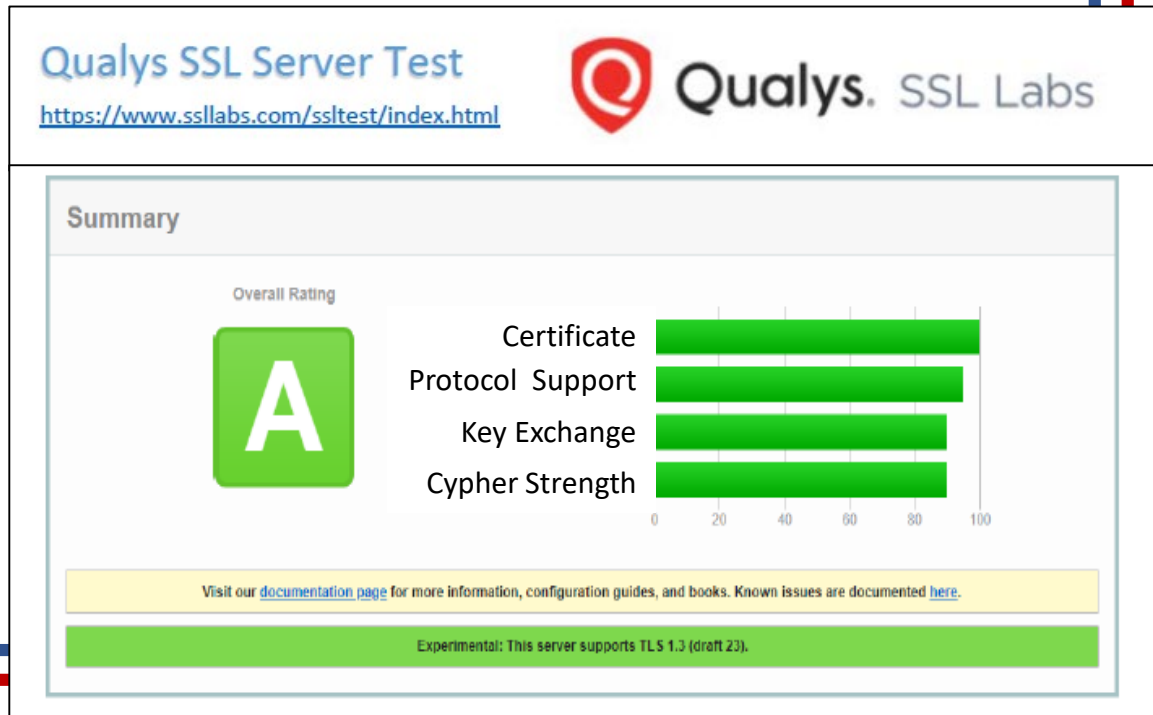
Implemented Solutions: LEARN Network



STEP 4:
UPGRADE THE CYRUS ONE 1006 Router

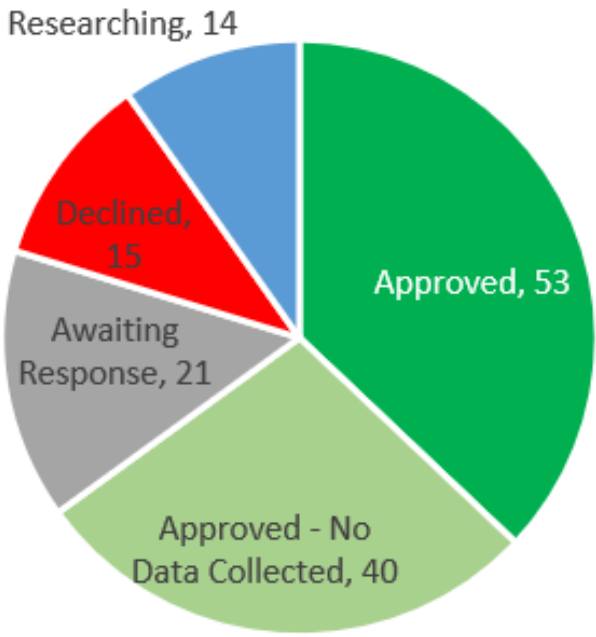
Implemented Solution: Resource Review

- Resources reviewed for security and privacy adherence
- Qualys SSL Server Test Results
  - rankonesports.com
    - Grade **F** -> **A**
  - sogosurvey.com
    - Grade **B** -> **A**
  - edgemakers.com
    - Grade **C** -> **A**
  - esgisoftware.com
    - Grade **B** -> **A**



Implemented Solutions: Resource Review

- Data Privacy Agreement
  - Data Privacy Agreement distributed to all software/website vendors utilized in the district.
    - Cypress-Fairbanks ISD version utilized April 2018 – November 2018
    - Approved to move to the Texas DPA utilized by the Texas Student Privacy Alliance



CFISD Resources

This database lists the vetted, approved, and declined resources that may be utilized by CFISD teachers and staff.

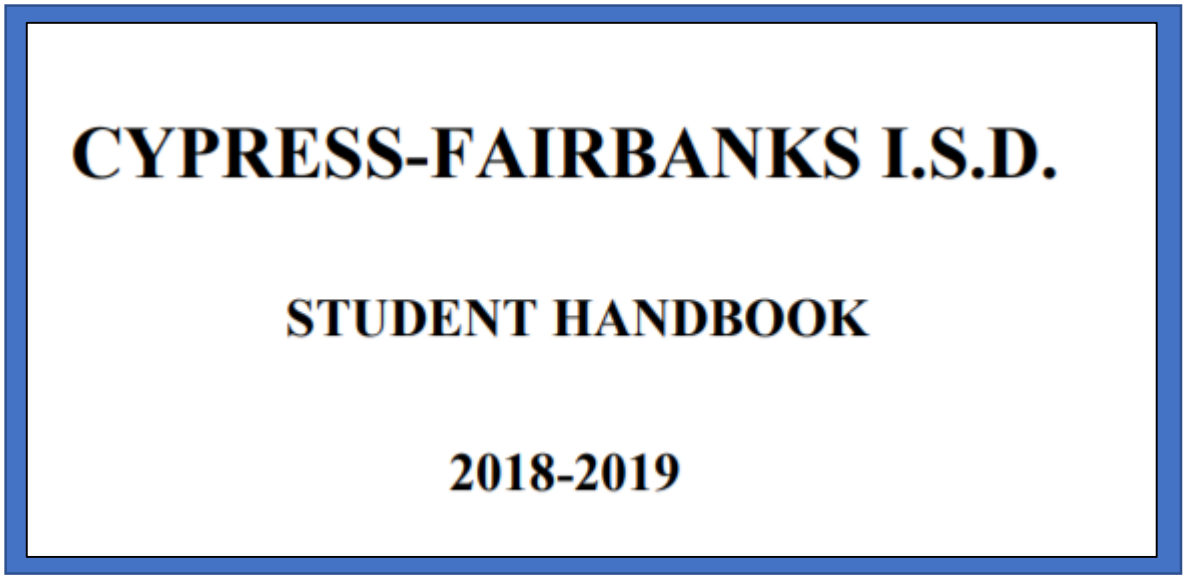
Status Key	**Approved:** Contract is signed and app is in use. **Approved w/ Guardian Release**: Guardians signed a contract to allow it to be used in a specific classroom with a specific group of students. **Not Approved:** Vendor was unable to sign the contract and, therefore, teachers are not allowed to use the app with students.

Items to Consider

1. Modify verbiage in the Student Handbook should be modified to ensure clarity regarding student login processes.
2. Require teachers to ensure the websites students are asked to review at home are accessible on the district network.
3. Require employees complete the Cybersecurity training distributed by Technology Services.

1 Student Handbook Review

- Modify verbiage in the Student Handbook should be modified to ensure clarity regarding student login processes.



1 Student Handbook Review

- Student Handbook – page HB-49
- SYSTEM ACCESS Access to the district's electronic communications system will be governed as follows:

Current

3. Students who are granted access to the district's system will be assigned individual accounts. Students are not to use a computer that is logged in under another user's name.

Advisory Suggestion

3. Students who are granted access to the district's system will be assigned individual accounts. Students are not to use an unattended computer that is logged in under another user's name.

Final Proposal

3. Students are not to use a computer that is logged in under another user's name unless that student is present and the use is part of a class assignment. Students should not use a device logged in as an employee.

2 Website Filtering and Utilization

- Teachers should ensure careful review of homework involving home internet utilization.
  - Vimeo
  - Youtube
  - Possible solutions

2 Website Filtering and Utilization

- Vimeo / Youtube
  - Accessible for employees.
  - Blocked for students at the URL and application control layers.
  - Issues occur when education applications use Vimeo to house videos.
  - Unblocking specific videos has not been successful and work-arounds contain additional risks.
  - Curriculum team working on alternative solutions to store video files.
  - Content Filter RFP

2 Website Filtering and Utilization

Desired Criteria:

- CIPA Compliant
- K12 Emphasis
- Integrated with AD
- Profiles based on AD Groups, subnets, machine type
- SSL Decryption
- Mobile and At Home Protection
- Entire School Year History available
- History should be exportable
- Custom Reporting
- Allows YouTube designated educational
- Website Overrides
- Reportable User Searches
- Real-time monitoring of user
- Educational Games Category
- URL and Application Control Blocking
- Customizable user notification/block pages
- Supports non-windows devices
- Supports multiple datacenters/ISPs with single history repository
- Supports large bandwidths and up to 300k devices
- Zero-minimum latency
- Network Peering Support (LEARN)
- Redundant
- Blocks Ultrasurf/Psiphon/proxies
- Adaptive alert capability – i.e. user has 30 porn blocks in last 15 minutes
- Industry/K12 recognized
- Up-to-date categorizations
- Option to block Unrated sites

3 Cybersecurity Training

- Require employees complete the Cybersecurity training distributed by Technology Services.
  - Training

Mouse Over Training

Number of Packages: 1
UPS Service: STANDARD
Weight: 5,0 KGS

Tracking Number: 1Z06E18A6840121864
Invoice Number: 323093 STAN
Reference Number 2: DEL TO C'NEE

http://wwwapps.ups.com/WebTracking/processRequest?HTMLVersion=5.0&Requester=NES&AgreeToTermsAndConditions=yes&loc=en_GB&tracknum=1Z06E18A6840121864&WT.z_eCTAid=ct1_eml_Tracking

3 Cybersecurity Training

Initial Introduction

KnowBe4 Cybersecurity Training Beginning September 7, 2018

Beginning Friday, September 7, 2018, you will receive an email notifying you of new cybersecurity training from KnowBe4. KnowBe4 is a third-party cybersecurity software used for security awareness training and simulated phishing attacks that helps us keep our electronic information safe. Once you click the link, you will be directed to a webpage with instructions to check your email inbox. A new email will appear in your email inbox with a unique secure link that does not require a password. The link provided will connect you to the training module.

Weekly Distribution

Dear JENNIFER MILLER,

Please see your **NEW** cybersecurity training module as part of this month's KnowBe4 cybersecurity training. The training will help equip you with the skills and knowledge you need to secure student, personal, and district data. The link provided will connect you to the training module, and will allow you to access the training as time permits.

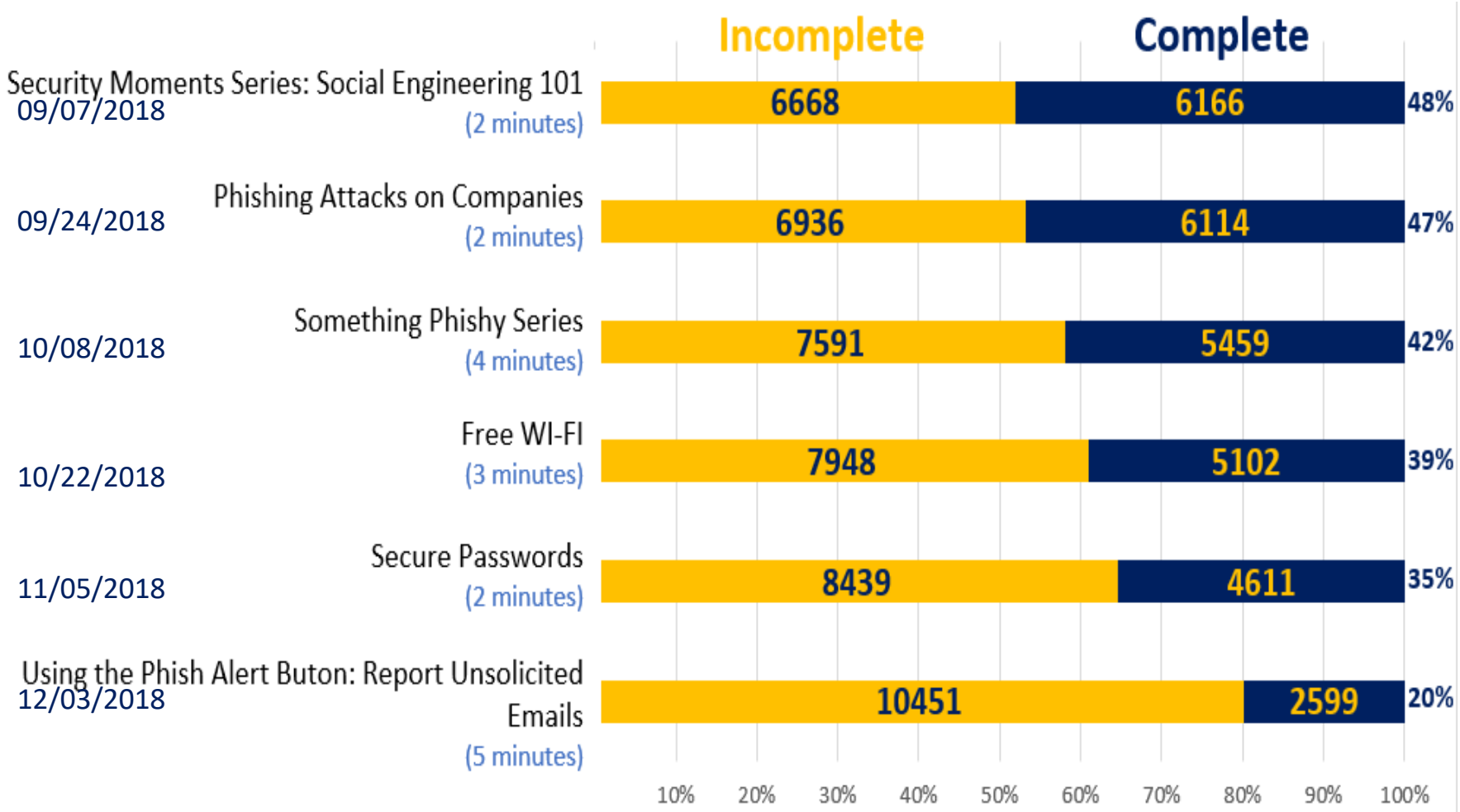
The courses you've been assigned are displayed below:

- Using the Phish Alert Button: Report Unsolicited Emails

Please use this link to start your training:
https://training.knowbe4.com/login/77b171100a0893/15d27190da4902

KnowBe4
Human error. Conquered.

3 Cybersecurity Training Participation



Suggestions to increase participation?

In Conclusion. . .

- Additional Concerns/Questions