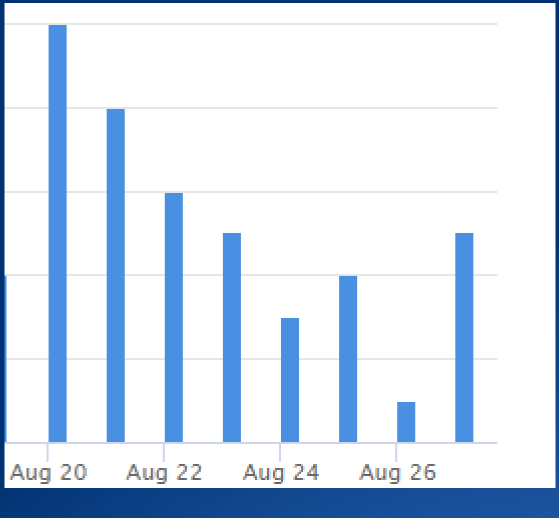
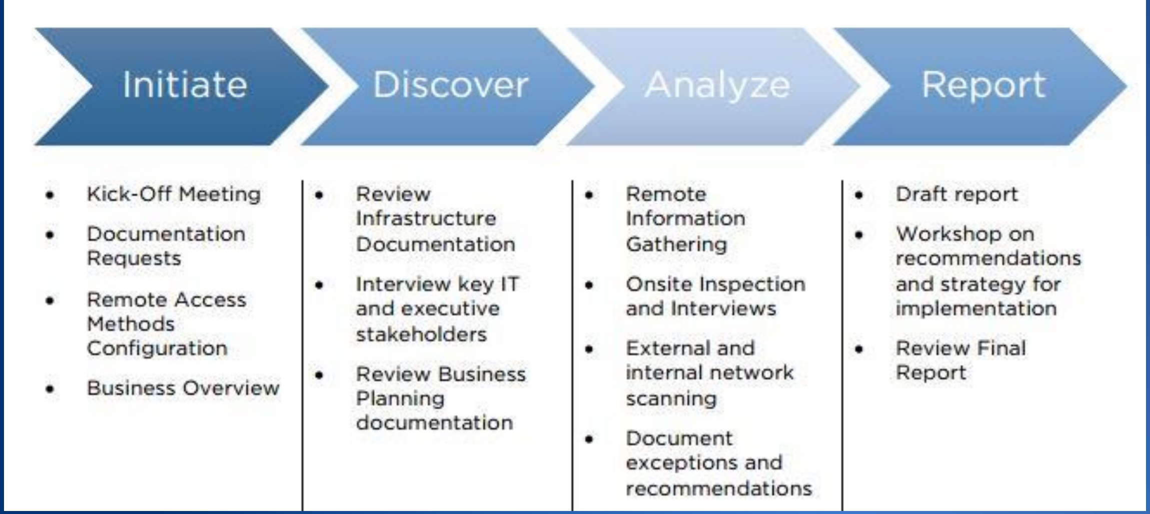
Cybersecurity Continual Improvements

- The week of **Monday, August 20th through Friday, August 24th,** was our first week with the newly implemented Phish Alert Button. The Phish Alert Button allows employees to easily report malicious email in order to remove the email from their inbox, and allow our Cybersecurity Team and email administrator to quickly and efficiently mitigate any risk associated with the emails. This was a fantastic move in improving our cybersecurity landscape.



- Audits are a part of any improvement plans, and on **Wednesday, August 22nd,** we spent time meeting with an external auditor to identify areas of improvement in our Information Technology Department. We received some great feedback and are looking at ways to continually improve.



Initiate

- Kick-Off Meeting
- Documentation Requests
- Remote Access Methods Configuration
- Business Overview

Discover

- Review Infrastructure Documentation
- Interview key IT and executive stakeholders
- Review Business Planning documentation

Analyze

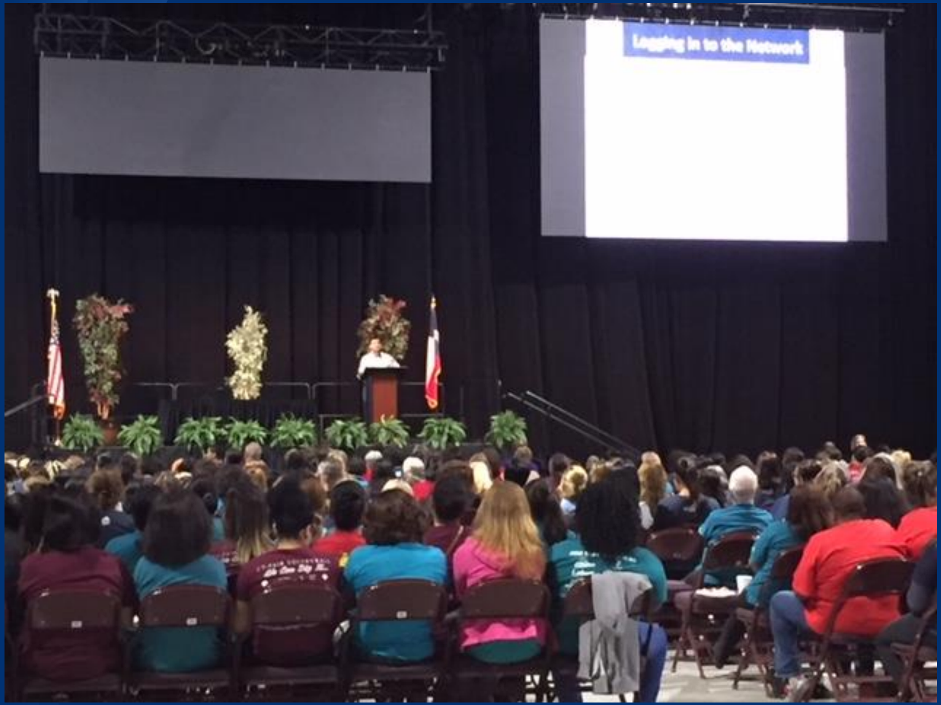
- Remote Information Gathering
- Onsite Inspection and Interviews
- External and internal network scanning
- Document exceptions and recommendations

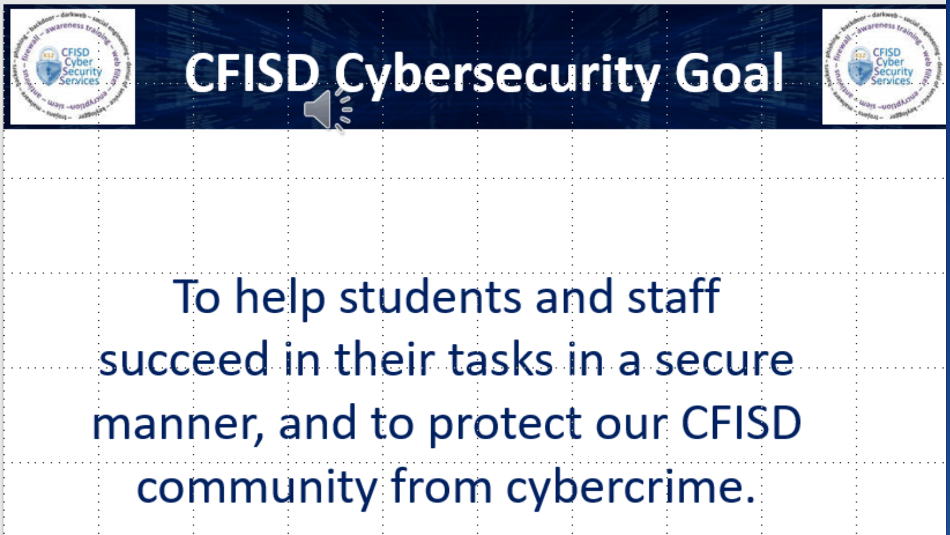
Report

- Draft report
- Workshop on recommendations and strategy for implementation
- Review Final Report

CFISD Cybersecurity Services
Posted by James Costello, Security Specialist, Technology Support Services – CCS 27 Aug 2018

Proper Procedure for Network Access





CFISD Cybersecurity Goal

To help students and staff succeed in their tasks in a secure manner, and to protect our CFISD community from cybercrime.

On Tuesday, August 21st, Eric Pina presented information nutrition services department regarding the proper way to access the district network. The presentation also stressed the importance of defense in depth security and complex passwords. Following the proper procedures for accessing a district computer, signing in to my.cfisd.net, and then logging in to Employee Access Center, ensures cybersecurity risks are mitigated. Screenshots and a live demonstration of accessing network email were also provided during the presentation. James Costello and Jennifer Miller were also in attendance to answer any additional security questions staff may have had regarding network usernames and employee access center.

Customer Care Center
Posted by Eric Pina, Customer Care Center Analyst

August 27, 2018

Other News on Cybersecurity

- T-Mobile confirmed that the telecom giant suffered a security breach on its US servers on **August 20** that may have resulted in the leak of "some" personal information of up to 2 million T-Mobile customers.

- The leaked information includes customers' name, billing zip code, phone number, email address, account number, and account type (prepaid or postpaid).

- However, the good news is that no financial information like credit card numbers, social security numbers, or passwords, were compromised in the security breach.

- According to a brief blog post published by the company detailing the incident, its cybersecurity team detected and shut down an "unauthorized capture of some information" on **Monday, August 20.**