Cybersecurity Improvements

Many data breaches, including the infamous Target data breach, are caused by a lack of security controls on the part of the vendor. This week, we continued conversations with CFISD vendors to ensure they are putting controls in place to protect CFISD data. The conversations were extremely fruitful, as our vendor representatives assured us that they would quickly work to remediate the issues which were addressed.

In order to ensure a security program continues to mature, it is vital to perform risk assessments on a regular basis. This week, we began talks with the Dept. of Homeland Security to identify tools and services they can offer to find and analyze our information systems. We are excited to work with them to leverage their expertise and to grow our IT Security program.

Given that most successful cyber attacks are a result of insecure passwords, we spent a lot of time and energy this week, assisting our employees with updating their passwords to a new strong password. As a general rule, passwords should be a minimum of 12 characters, include uppercase, lowercase, numbers, special characters, and not be a dictionary word.

Trusted Learning Environment (TLE) Completed on Monday, May 9th, 2018

James Costello, Eric Pina, Jennifer Miller, and Frankie Jackson met on Wednesday May 9th at noon to complete the final review of the district Trusted Learning Environment (TLE) application. With over 175 items of evidence, the team compiled data into 25 narratives to submit to the Consortium for School Networking (CoSN) for evaluation. The district has worked on this project for 2 years. This team has focused specifically on this project for the last 6 months. This completed work does not signify the end of the project, but now the real work of continuing to work with vendors and district personnel to continue to train and support the district's cybersecurity and data privacy initiatives. This team has learned so much together. The possibilities for our team are limitless.