2/6/23 YPICS TECHNOLOGY BOARD REPORT

DOCUMENT TABLE OF CONTENTS:

SUMMARY

The YPICS Tech Team this year is taking a deep dive into cybersecurity and putting in place various systems and policies to help ensure that we do everything we can to avoid a cybersecurity incident. Below is a brief summary of the various items that we have put in place during the first semester as well as a list of future projects for the second semester.

IMPLEMENTATION OF 2-STEP VERIFICATION

This last October we expanded our use of 2-Step Verification for our Google accounts to all YPICS Staff members. Prior to October of 2022 we required 2-Step Verification for all YPICS Administrative staff.

We expanded 2-Step Verification to all staff to help combat against the most common forms of cyber attacks since it requires additional information beyond a username and password. If a username and password is compromised, the account is still secure as long as the attackers do not gain access to the 2-Step Verification method. We also expanded our usage of 2-Step Verification in anticipation for the renewal of our cyber

insurance plan. The current trend in the cyber insurance industry is to require some form of Multi Factor Authentication to qualify for insurance. Our current provider does not require this but we wanted to make sure we are ready in case they start requiring some form of MFA.

In addition to requiring 2-Step Verification for YPICS Google Accounts, all YPICS Tech Team members are required to use Multi Factor Authentication for any system that we use. This was done to help make sure that our main administrative accounts are secure and not easily accessible by non YPICS Tech Team Members.

MS-ISAC

To help be better prepared for cybersecurity threats, the YPICS Tech Team recently joined the Multi State Information Sharing and Analysis Center (MS-ISAC). MS-ISAC is a federally funded division of the Center for Internet Security. Membership is free for any state, Local, Tribal, and Territorial entity which includes K-12 education institutions.

As a member of MS-ISAC YPICS is gaining free access to the following services:

- A 24 hours a day, seven days a week, 365 days a year Security Operations Center (SOC)

  The MS-ISAC SOC monitors our public IP addresses to look for signs of compromise or malicious activity. If YPICS was to experience either of these issues the SOC would notify the Director of Technology so action can be taken in a timely manner.

  The SOC will notify us if any YPICS account is found in a data breach and is compromised. This will help the YPICS Tech Team take the appropriate steps for securing the compromised account.

  The SOC also sends the YPICS Tech Team email alerts when there are known vulnerabilities in tech programs that YPICS staff use. The YPICS Tech Team uses this information to push out updates and inform staff of when they need to upgrade their software.

- Malicious Domain Blocking and Reporting (MDBR)

  This program helps proactively block known malicious domains. The program also provides the YPICS Tech team a weekly report of malicious domains that have been accessed from our network. This information is helpful for identifying what domains MBDR is not blocking that the team needs to internally block on our web filter.

- Cyber Incident Response Team (CIRT)

  If YPICS was to experience a cybersecurity incident we can contact the CIRT for help with how to respond to the incident. The CIRT also helps with making sure that our remediation efforts are effective.

- Malicious Code Analysis Platform (MCAP)

  The MCAP platform is used to submit and analyze suspicious files and URLs. The YPICS Tech team uses this platform to make sure that a suspicious file or URL is safe before opening it on our laptops.

These are just a few of the services that the YPICS Tech Team has signed up for. A full list of free and paid services that MS-ISAC offers can be found on their website. While we know that it is impossible to avoid all cybersecurity threats, we hope that having these additional free services in place help increase our security posture and help us avoid any incidents.

IMPLEMENTATION OF CIS IMPLEMENTATION GROUP 1

After researching various cybersecurity frameworks, the YPICS Tech Team decided on starting with the Center for Internet Security (CIS) Implementation Group 1 (IG1) recommendations. CIS has identified the controls in IG1 as “essential cyber hygiene” that all organizations need in place to set a foundational set of cyber defense

safeguards to guard against the most common attacks. A full list of CIS Implementations can be found on their website.

IMPLEMENTATION OF MOSYLE DETECTION & REMOVAL

Mosyle Detection & Removal is a part of our Mobile Device Management (MDM) platform. Detection & Removal scans all YPICS macOS devices and if the program identifies known malware it will quarantine the file and alert the tech team so we can manually review to see if the file is safe or needs to be deleted off the machine. If the file needs to be deleted we can take action remotely through the Mosyle platform.

SECOND SEMESTER PLANS

Below are a few of the projects that we are currently working on to continue to strengthen our cybersecurity at YPICS.

- Implementation of our new YPICS Password Policy
- Continue to implement CIS Implementation Group 1
- Start phishing simulation campaigns to help build staff awareness to phishing
- Create a staff training plan about important cybersecurity topics that everyone needs to know.