Information Security
TDPAC Update
Fall 2019
Fall 2020
InfoSec Goals

Focus on real world threats

Provide transparency for all stakeholders

Focus on communication

Secure through partnerships (we have failed if we say no)
Increasing Threats with Real Consequences

- More targeted attacks against K12
- Systems used by K12 are becoming more complex
- There is an increasing amount of competing priorities
- Compromises are highly publicized
App used at high school in Highlands Ranch rewards students for turning their phone off in class

HIGHLANDS RANCH, Colo. -- As a teacher at Mountain Vista High School in Highlands Ranch, Jason Cochrane has seen cell phones distract kids during class.

"Over the years cell phones have definitely started to disrupt some of the time, or the educational time, I would like to have with those kids," he said.

So now he uses an app called Pocket Points, to help minimize those disruptions in class.

"It monitors how much non-use they have of their cell phone," Cochrane said.

Many teachers ask students to leave their phones in a phone holder at the front of the room, but Cochrane didn’t want to be responsible for any damage. So he uses the app to motivate students to just turn their phones off.
What are we Seeing?

- Phishing attacks
- Crypto mining
- Drive By downloads
- Partner data loss
- Privilege abuse
- Student misuse
What are we Doing?
Hygiene
Log Management

- Splunk gathers 600 gigs of logs per day
- Our log management is resigned to respond to “the pivot”
- We have alerting set up to monitor activity related to phishing and privilege escalation
- We are looking into more granular log collection for administrative features using powershell and what log management looks like in the Cloud
Monitoring

☐ This is why we have an InfoSec team
☐ We actively monitor
  ☐ Firewall logs
  ☐ AV system
  ☐ Email system
  ☐ Privileged use
  ☐ Google Cloud
☐ InfoSec monitoring provides consistency
Software Vetting

![Graph showing software vetting results by quarter from Q1 16-17 to Q4 18-19. The graph includes bars representing the number of approvals, approvals with restrictions, and denials.]

- **Denied**
- **Approved with Restrictions**
- **Approved**
Incident Response
Looking Back
Chromebook Transparency

- Looking to maintain trust with the community by offering the following to families
  - Student monitoring
  - Access control on non-district networks
  - Offering dashboards to school leaders as well
Phishing Awareness

- We dedicate 1/2 to 2/3 of an FTE to phishing mitigation
- We have developed processes to respond to common threats
- We are working with our email gateway provider to offer targeted training throughout this year
Next Generation AV

- We have been historically successful at responding to advanced threats.
- The environment is increasingly complex.
- We are working to bring down MTTD and MTTR.
- Our goal is to find a solution that will help us quickly respond to ransomware attacks.
Future InfoSec teams will have more of a focus on:

- Identities - how to consistently manage access to data on hundreds of cloud applications?
- Data - how do we inventory data at its source and respond to threats like abuse, privilege escalation, and data exfiltration without compensating controls?
- Integrations - how do we secure the APIs and other frameworks required to share data throughout interconnected systems?
Looking Ahead
Renewed Hygiene Efforts

- Chromebooks and security controls on Windows desktops are protecting our users while applications and integrations continue to increase in complexity.

- We are working to increase security of core infrastructure by:
  - Codifying baseline configurations and exceptions
  - Reviewing processes and technologies that separate: dev, test, and prod.
  - Reviewing administrative access
Cloud Infrastructure Security

- COVID has accelerated infrastructure’s move into the cloud.
- The InfoSec team is involved to ensure we are protecting data and infrastructure as we explore:
  - VDI in the Azure cloud
  - O365 for staff
  - Infrastructure as a service in the Azure cloud
  - Power BI and Power Apps
Review of Services offered to Schools

☐ Our network is primarily designed to support Windows AD connected devices

☐ Most of our devices at schools are now Chromebooks, IOT, or STEM

☐ That creates unnecessary attack surface area for threats like ransomeware and APTs

☐ We are just beginning to have conversations with the goal of increasing flexibility for schools and decreasing risk for business systems