21-22
Information Security Update
Meeting Goals

- Provide high level transparency.
- Gain feedback especially related to communications and student tech use.
- Look for gaps.
- Look for areas of interest from the committee.
Team Goals

- Focus on real world threats.
- Provide transparency for all stakeholders.
- Focus on communication.
- Secure through partnerships.
Team Structure
Threat Landscape
Evolving Technologies

- Shift from Active Directory connected Windows devices at schools to Chromebooks and specialized labs.
- Increasing need for data and systems integrations.
- Shift from on prem hosting to cloud services for productivity apps such as Google and Microsoft.
- Increasing need for IoT devices and building automation.
- Gradual shift to a more mobile workforce.
Advanced and Targeted Attacks
K-12 Specific Watering Hole Attack

● Our advanced endpoint protection system began alerting on numerous instances of SocGholish on teacher workstations across the district.
  ○ The number of cases and timing indicated that further investigation into a root cause was necessary
● Investigation indicated the following:
  ○ Jeffco staff members received emails from a compromised vendor account
  ○ The emails directed staff members to a compromised section of a standardized testing providers website.
  ○ Code on the site attempted to download a stager then C&C.
  ○ Further analysis of our logs indicated that a widely used curriculum website was also compromised.
● Jeffco staff worked with vendors on response and remediation efforts.
  ○ No student data on the vendor (or Jeffco) systems were compromised.
Targeted Attack against our password reset system

- Started with a few users complaining of email setting changes and account lockouts.
- Later in week 1 we identified about 10 accounts that were exhibiting the same behaviors: password changes, account lockouts, email settings changes.
- We then used logs, firewalls, and O365 configuration changes to play IP whac-a-mole with the attacker.
- Support system logs indicated that much of the malicious activity was centered around our password reset system.
- Detailed review of the application logs indicated the attacker was using a vulnerability in our account provisioning process to change user passwords.
- InfoSec worked with IDM, HR, and application owners to change the process (during winter hiring season).
Evolving Threats

1. Ransomware
2. Phishing
3. Student Tech Misuse: *Relationships, Inappropriate Content, Account Theft, Hacking*
4. Advanced Persistent Threat
5. Browser Based Threats: *Drive By, Malvertising, Crypto*
6. Staff Tech Misuse
7. System Integration Vulnerabilities
8. Partner Breach/Data Loss
9. Traditional Infrastructure *Malware, DoS, Misconfiguration, Botnet*
Celebrations

Device + Digital Tool = Successful Jeffco Graduate
Celebrations & Opportunities

- Increasing device usage
- FCC & ESSR Funding to solve for Digital Equity
- Advisory Teams to increase Collaboration & Transparency
  - TechForEd Advisory Team & Steering Committee
  - Library Advisory Team

Grow
- Partnerships
- Collaborations
- Vision

TechForEd Expansion Challenges
Student Tech Misuse

- Increasing device usage
- Lots of change with staffing
- Competing priorities for student, staff, and admin training
- Student Behaviors vs Solving with Technology
- Technologies for reactive accountability

Opportunity to:
- Redesign Digital Citizenship
- Conversations with Parents & Community about Tech use
- Redesign Ed Tech role to support the challenges
Ransomware

- K-12 = easy targets
- Attack vectors are increasing
- Many attacks involve APT
- Jeffco’s tech is transitional
- Large number of end users
- Technology is more complex
- IOT growth

- Increased use of cloud such as Google and O365
- Chromebook adoption
- Advanced endpoint protection
Phishing

- Public facing organization
- Large number of users
- Vulnerable sector
- Cost vs. benefit for attacker is great
- Types of attacks are limitless

- Well defined response process
- Great district support for quick drastic mitigation efforts if needed
- Strong end user awareness
- Solid business process containing attacks
- Industry standard technical tool set
Advanced Persistent Threat (APT)

- Incredibly porous network
- Incredibly diverse technologies
- Lack of staffing (this is true across the industry)
- Increasing number of integrations
- Diversified working environments
- Moderate process maturity

- Advanced endpoint protections
- Increasing configuration consistency
- Strong relationships and info sharing throughout the district
- Log collection and correlation for detection and response
- Network and role compartmentalization
Browser Based Threats

- Weak sector
- Diverse working environments
- Inconsistent staff skillset

- Defense in depth level of tools
- Organizational support for drastic response strategies
Staff Tech Misuse

- Poor data culture
- Immature application landscape
- Inconsistent staff skillset
- Inconsistent data sharing practices within the district and between our partners
- Siloed practices

- Strategic data goals
- Desire to build well defined systems and practices
- Starting to align architectural goals with district strategies
System Integrations

- Poor oversight (Siloing)
- Lack of standards
- Lack of consistent development practices
- Exploding need
- Highly varied partner experience

- Great contractual oversight
- Generally accepted best practices are in place and understood
Partner Data Loss

- Large number of partners
- InfoSec oversight is limited to questionnaire and contract review
- Lack of national standards
- Phycology of incident management
- Great contractual oversight
- Generally accepted best practices are in place and understood
Infrastructure

- Large network attempting to support a diverse set of needs
- Culture that values tribal knowledge
- Transitional times lead to poor hygiene
- Great relationship between core teams
- Generally accepted best practices are in place and understood
Focus on the Pivot

Defining principle embedded into all the InfoSec team’s activities.
Question

Name all the ways a spammer could try to trick a Jeffco employee?

..... There are 1,000s
Better Question

What will a spammer likely do after they trick the employee?

- Utilize resources (people, compute, money, things)
- Move laterally around the system/network
- Escalate privileges
- Exfiltrate data
Primary Services

- Project involvement
- Compliance
- Software vetting
- Training, partnerships, awareness
- Incident Response
- Policy creation
- Legal support
- AV oversight
- Edge protection
- Web filtering
- Log management
- Configuration oversight
- Vulnerability management
Vulnerability Management
Threat Management

- Malware: 3804
- Exploit: 1822
- Persistence: 706
- Lateral Movement: 415
- Execution: 258
- Tampering: 173
- Discovery: 109
- Command and Control: 104
- Privilege Escalation: 93
- Initial Access: 29
Software Vetting

2019-20
Blue

2020-21
Red

2021-22
Yellow

Chart showing data trends from 2015 to 2022.
Areas of Focus
Into the 22-23 School Year
Communications

- Our people are our best partners for detecting and responding to threats
- COVID distracted us for a couple years
- Leadership changes will require us to revisit topics
- Goal is to create a hub to share information, build excitement, and share real world knowledge.
- What would you like to see us communicate better?
Process Retooling

- **Splunk Log management system**
  - Goal of the system was to respond to human threats.
  - Google, Microsoft, Cortex, and shifts to the cloud require an evolution.

- **Software vetting**
  - Software vetting process is **very labor intensive** and does little to mitigate against partner data loss.
  - Revised process will focus on the number of tools and current threats.

- **Incident response**
  - How can we delegate student based response to schools while maintaining consistency?
  - Do we feel comfortable delegating some technical oversight to school leaders?

- **Vulnerability management**
  - We are naturally evolving away from configuration/patch prioritization into strategic conversations.
  - Looking into more of a self-service model with oversight.
Standardization

- Continue to build on infrastructure standards with a focus on codifying configurations and automation.
- Define integration standards focusing on supporting ed tech tools and cloud flexibility.
- Define identity standards focusing on ed tech tools, cloud flexibility, and data access.
- Define data ownership, lifecycle, and inventory standards.
Architectural Strategy

- Define key roles and responsibilities.
- Identify and socialize: individual team goals, team practices, toolsets.
- Look for opportunities to build efficiencies and remove duplicated efforts.
- Integrate architectural work with project management processes and change management.
- Define strategy with a focus on tech plan alignment, redefining school network services, modernizing and streamlining identity management practices, building a data strategy.
Data Strategy

- Define and reinforce basic governance principles (ownership, inventory, lifecycle, sharing).

- Standardize processes that feed key systems and build feedback mechanisms for continual improvement.

- Identify and socialize reporting functionality that is overlooked and underutilized in our current apps.

- Define and build transform processes and centralized data structure to support advanced reporting, analytics, and integrations.