1. Defense in Depth Review
2. 2017 Annual Cyber Security Report (ACSR)
   • Threat Landscape
   • Highlights
   • Concerns
Defense in Depth (InfoSec Roadmap)

Network
- Network Access Control (NAC)
- F5 Upgrade and Application Firewalls
- Dark Web/Anonymizers
- SandBlast
- CheckPoint Firewalls
- Network Zones (DMZ, DDC, InfoSec, etc.)

Network Redesign Project (NRP)
- Not Started
- In Progress
- Done/Ongoing

Servers
- NSX/Microsegmentation
- Tenable Vulnerability Assessment
- DDC Server Support Strategy & Password Manager Pro
- Server Zone Migration & Separation of Environments (SOE)
- 24/7 Network Operations Center
- Data Center Security & Facilities

Virtualization (VMWare)
- VMWare

End Points
- JAMF & Apple End Point Management
- DUO 2-Factor Authentication & Secure VPN
- McAfee End Point Protection
- Patch Management
- High Value Workstation Support
- Access Control & Separation of Duties (SOE)

Active Directory
- NCSAM

Data
- "Data at Rest" Strategy
- "ED to AD" & SHA-2 Password Encryption
- Virtru Email Encryption
- Banner Data Defense
- Google Security
- Consolidated Backups

Forensics
- Splunk SBM
- MalwareBytes
- EnCase eDiscovery
- Network & Server Monitoring (SolarWinds, Apcon, Extrahop)
- Google Analytics & CheckPoint Reporting
- Incident Management (JAR, Red Flag, etc.)

Cyber Team
- Cyber

People
- NCSAM
- Communication (Message from CIO, Phishing Videos, etc.)
- Compliance Programs (Red Flag, PCI, Penetration Testing, NIST)
- Policy: ISP & AUP
- Educate Leadership (Regulatory Compliance, etc.)
- Engage Board of Directors

Access Control & Encryption
- Access Control & Encryption

Cyber Security
- Cyber Security

IT Staff Engagement (Program/Roadmap, Annual Cyber Security Offsite, Management Buy-In, etc.)

People
- People

CIO Priority
- CIO Priority
2017 ACSR: Threat Landscape

1. Largest losses to date globally: identity & financial
2. Higher Education is #3 target (after Finance, Healthcare)
3. Increased regulations & laws: PCI, GDPR
4. Equifax! Uber, Google Ole…
5. New threats: WannaCry, Kaiser, Hidden Cobra
6. Increased Sophistication: phishing, BEC, etc.
7. FAFSA (Application for Federal Student Aid) - 20 to 80 million students' records
8. North Korea, Russia, China and India are worst state offenders
2017 was PCC’s “best year ever”:

2. Established Red Flag committee
3. Gartner IT Score: 3.1 to 3.8
4. No reportable events (defended against new threats: WannaCry, etc.)
5. Completed NIST “dry run” – audit in Q1 2018
6. 2nd Annual “National Cyber Security Awareness Month”
7. Encryption of PCC’s “system of record” (Banner data Defense)
8. Implemented district-wide Patch Management
9. Began implementation of Splunk SIEM
10. Virtru email encryption for the Dental Division (HIPAA protection)
11. Expanded network and server monitoring capabilities

All *keystone* objectives identified in last year’s report (e.g. block USA dark sites and outbound traffic, implement Sandblast, Banner Database Encryption, etc.) were successfully met.
2017 ACS Report: Concerns

1. REN-ISAC\(^1\) Dark Web database
2. Google's Ole breach
3. Dropbox, Yahoo, other cloud services breached throughout 2017
4. North Korean “Hidden Cobra”
5. Chief Information Security Officer (CISO)
6. Budget

\(^1\)The Research and Education Networking Information Sharing and Analysis Center (REN-ISAC) serves the entire EDU space in the United States: “In this role, we work with trusted third parties to notify higher education institutions of infected hosts and suspicious network traffic.”
Questions?

Michael Northover, CIO