Cybersecurity Audit Review

Connection to Strategic Plan 2021-2025:

Demonstrate stewardship by allocating resources effectively and equitably.

Chris Fahnoe – Director of Technology
March 2023

This presentation will cover:

1. A landscape of ongoing cybersecurity threats

2. Viewing cybersecurity as a team

3. Getting a comprehensive external view

4. A general review of the audit

5. Implementation plans

BACKGROUND OF AUDIT

Cybersecurity Landscape

In the last 3-5 years there is a noted increase in:

- Ransomware
- Phishing attacks
- Malware
- Password attacks
- Denial of Service (DDoS) attacks

Cybersecurity as a Team

Takes a team to build a culture:

- Board of Education
- District leadership
- Tech25
- Building leadership
- All end users

Cosmopolis

- Comprehensive Penetration Test
- Enterprise Risk Assessment
- Enterprise Incident Response Program

Overall Feedback

Letter of Attestation lists that:

- District 25 has in place the elements for a Culture of Cybersecurity
- Low incidence of actional vulnerabilities
- Up-to-date systems and technology
- Low incidence of default login credentials
- A thoughtful and detailed network

IMPLEMENTATION

Implementation Areas

Account Management
- Multi-factor authentication & password complexity
- Account access – least privilege

Vendor Management
- Requesting cybersecurity profile
- Data privacy agreements for all vendors with personal data

Network Monitoring and Backups
- Exploration of recommended tools
- Continuation of redundant, multiple site backups

Implementation Areas

Procedures
- Incident response
- Data breach
- Annual Reviews
- Patching and updates

User Training and Awareness
- Phishing campaigns
- Password management and malware

Beyond the Audit

Membership and Resources

- Consortium for School Networking (COSN)
- Multi-State Information Sharing and Analysis Center (MS-ISAC)
- Cybersecurity and Infrastructure Security Agency (CISA)
- K-12 Security Information Exchange
- Cyberpools

QUESTIONS?