Protecting Public K-12 Education Data from Cyberattacks: Lessons from Alabama
Alabama’s Recent Cyberattack Events

- July 2019 (Houston County Schools) – Impacted telecommunications, Internet service, and computers connected to the WAN causing a delay in school opening.

- November 2020 (Huntsville City Schools) – Impacted some personally identifiable information, emails, and contractors who performed services for the district.

- May 2021 (Madison City Schools) – Threat identified by advanced threat protection systems as a possible breach.
Alabama’s Lessons Learned

- Lack of awareness to the impact cybersecurity attacks have on school systems
- Improperly maintained equipment and security protocols
- Insufficient training related to cyberthreats and attacks for all employees
- Inability to properly audit network environment
- Missing management for mobile devices and non-district devices
- District size isn’t a factor in being targeted
- Upgraded need for early detection software and tools
Alabama’s Response - ALSDE

Reporting
- Contact ALSDE, Service Provider, Local law enforcement

Actions taken by the ALSDE
- VPN Tunnel Disabled (State Enrollment Disabled)

Mitigation / Confirmation
- Letter from LEA Superintendent

Service Restoration
- VPN Tunnel Enabled (State Enrollment Enabled)

Network Security Improvement Suggestions
- Training, Software, Password Policy, Backups
Initially most funding for Cybersecurity was provided by local funds. This created a great deal of variance in the levels and types of protection.

- During the 2021 Legislative session state funding was appropriated to assist school systems in upgrading equipment and resources. Approximately $25,000 per LEA.

- Based on both, success and need identified, the legislature increased the appropriation to approximately $68,000 per LEA in the 2022 session.
The Alabama State Department of Education partnered with Alabama Leaders in Education Technology (ALET) to develop an application that all school systems must submit prior to funding.

- Application questions assessed things such as:
  - What the environment is composed of - number of users, types and quantities of devices, etc.
  - Network structure
  - Existing security resources - hardware, software, staffing
  - Best practices in use

- The application consists of approximately 100 questions which provides detail of each system’s current state and intended use of funds.

- All applications were submitted electronically using software that encrypted the data in transit and kept it encrypted in place.
Alabama’s Response – ALSDE & ALET

<table>
<thead>
<tr>
<th>Best Practice/Key Resource</th>
<th>2021</th>
<th>2022</th>
<th>Improvement/ Change</th>
<th>Improvement Attributed To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup Method (3-2-1)</td>
<td>36%</td>
<td>35%</td>
<td>-1%</td>
<td>Training/Staff</td>
</tr>
<tr>
<td>Backup Testing</td>
<td>54%</td>
<td>60%</td>
<td>5%</td>
<td>Training/Staff</td>
</tr>
<tr>
<td>Unsecured RDP Permitted</td>
<td>15%</td>
<td>24%</td>
<td>9%</td>
<td>Training/Staff</td>
</tr>
<tr>
<td>Uses VPN for Remote Connections</td>
<td>85%</td>
<td>85%</td>
<td>1%</td>
<td>Training/Staff</td>
</tr>
<tr>
<td>Network Segmented</td>
<td>92%</td>
<td>91%</td>
<td>-1%</td>
<td></td>
</tr>
<tr>
<td>Server Segmented</td>
<td>61%</td>
<td>60%</td>
<td>-1%</td>
<td></td>
</tr>
<tr>
<td>Guests Segmented</td>
<td>62%</td>
<td>70%</td>
<td>8%</td>
<td>Training/Staff</td>
</tr>
<tr>
<td>Win Admin Access Restricted</td>
<td>57%</td>
<td>69%</td>
<td>12%</td>
<td>Training/Staff</td>
</tr>
<tr>
<td>Server Profiles Deleted</td>
<td>21%</td>
<td>57%</td>
<td>36%</td>
<td>Training/Staff</td>
</tr>
<tr>
<td>Server Tasks Not Run Under Named User</td>
<td>58%</td>
<td>63%</td>
<td>5%</td>
<td>Training/Staff</td>
</tr>
<tr>
<td>Win Updates Automated</td>
<td>64%</td>
<td>54%</td>
<td>-10%</td>
<td>Training/Staff</td>
</tr>
<tr>
<td>User Password Policy</td>
<td>84%</td>
<td>90%</td>
<td>6%</td>
<td>Training/Staff</td>
</tr>
<tr>
<td>Anti-Spoofing Settings</td>
<td>27%</td>
<td>70%</td>
<td>43%</td>
<td>Training/Staff</td>
</tr>
<tr>
<td>Multi-Factor Authentication</td>
<td>30%</td>
<td>72%</td>
<td>41%</td>
<td>Funding</td>
</tr>
<tr>
<td>Employee Training Implemented</td>
<td>47%</td>
<td>93%</td>
<td>46%</td>
<td>Funding</td>
</tr>
<tr>
<td>Uses MDM to Manage Mobile Devices</td>
<td>63%</td>
<td>90%</td>
<td>27%</td>
<td>Funding</td>
</tr>
<tr>
<td>Has Incident Response Plan</td>
<td>6%</td>
<td>85%</td>
<td>79%</td>
<td>Training</td>
</tr>
<tr>
<td>No Legacy Devices</td>
<td>42%</td>
<td>49%</td>
<td>7%</td>
<td>Funding</td>
</tr>
<tr>
<td>Systems using free CISA Services</td>
<td>22%</td>
<td>73%</td>
<td>51%</td>
<td>Training</td>
</tr>
</tbody>
</table>

Key Performance Indicators collected through the application submitted by LEAS demonstrates improvement in most areas.
Alabama Achieves

Breakdown by percentage of how appropriated funds are being utilized to combat cyberattacks.

Percent of Funding Use

- Salary-Related
- Contracted Services
- Antivirus
- Backup Improvements
- Intrusion Detection
- Content Filter
- HW Upgrade
- Training
- Firewall
- Other
- MFA Authentication
- Spam Filter
- Mobile Device Management
- Penetration/Vulnerability

2021 vs. 2022
• Ensuring that all staff are annually trained in prevention.

• During 2022 the first cyber camp was hosted at Troy-Montgomery campus with invitations to LEA Technology Directors and network staff.

• ALET works collaboratively with CISA to ensure that government and industry experts provide leading edge training to LEA Technology Directors and Network Administrators.

• ALET will be hosting two annual cyber camps moving forward.

• ALSDE is furthering their partnership with ALET to support a certification program for Technology Directors via the University of Montevallo.
Brandon Payne, Ed.D.
Deputy Superintendent
brandon.payne@alsde.edu
(334) 694-4906