

Cybersecurity Readiness in Maryland's Education System: A Brief Overview

Scope of the Problem:

- The K12 Security Information Exchange estimates that there have been more than 1,330 publicly disclosed cyberattacks since 2016.
- In the last three years, two large school systems have suffered cyberattacks, which affected almost 250,000 students and cost millions in recovery.

State Standards and Readiness Assessment:

- The Maryland DOIT has established Minimum Security Standards for state agencies, including Maryland Local Educational Agencies (LEAs).
- In 2023, a survey was conducted with the LEAs to assess their readiness and hindrances to implementation. Of the 24 LEAs, 15 responded in various sizes.

LEA Readiness Survey Results:

- Snapshot of Schools Responding
 - 46.7% of respondents were schools between 10,001 - 49,999 students
 - 33.3% of respondents represented schools with 50,000+ students
 - 20.0% of respondents were from schools with less than 10,000 students.
- How many schools have utilized basic cybersecurity protection procedures?
 - Multi-Factor Authentication
 - 53% use some level of MFA
 - 27% had enabled MFA for all employees
 - 20% do not use MFA at all
 - Endpoint Detection and Response and Network Monitoring
 - Only 27% of LEAs felt they had adequate network monitoring and endpoint detection capabilities.
- How many LEAs felt they met the DOIT minimum standard?
 - 0%
- What resources will LEAs need to meet the standards?
 - For 22 CSF/NIST Categories in the State Minimum Security Requirements, 15 LEAs pointed to **Staffing and Skill Set/Training** as the biggest hindrance

How will SB0981 address this problem?

1. It will set an achievable starting point by prioritizing the highest value measures and supplying centralized support to achieve them.
2. It will require MFA, endpoint detection, and network monitoring of all LEAs.
3. Implements additional support for LEAs under the direction of the Director of Local Cybersecurity.