K12 Security Advisory Guidance for Improving Cybersecurity in Mississippi School Districts

Information Security, or Cybersecurity, is a dynamic, ever-evolving field. The days of a school district addressing its data security concerns through the purchase of fireproof cabinets have given way to fighting daily online attacks from overseas parties. The emergence of new threats is happening in a world where near-instant access to student and district information is expected not only by school employees, but also by a broad group of stakeholders. Layer into this the need to protect student data under the terms of federal laws such as the Family Educational Rights and Privacy Act (FERPA), the Children's Online Privacy Protection Act (COPPA) and the Protection of Pupil Rights Amendment (PPRA), and the complexities of school districts' cybersecurity status can seem overwhelming.

Mississippi school district personnel wrestling with cybersecurity challenges have expressed their desire for guidance from the Mississippi Department of Education (MDE). In response, and in cooperation with district technology directors, MDE's Office of Technology and Strategic Services (OTSS) has created a guidance document to advise district administrators, technology directors, and staff on these issues.

The MDE will develop additional chapters in the coming months, growing the list of resources and links that address each subject matter area. Each chapter will guide districts as they develop and implement a comprehensive Cybersecurity Plan.

This guide also serves as a companion to MDE's Cyber Awareness Webinar series, which is available on the Information Security and Data Privacy webpage (link below). Please check that page regularly for guidance document updates and new webinar postings.

Information Security and Data Privacy | The Mississippi Department of Education (mdek12.org)

MISSISSIPPI DEPARTMENT OF EDUCATION

Chapter 1. "To Know"[1]: What is Your Cybersecurity Posture?

Introduction: The focus of this chapter is the need "To Know" the current state of cybersecurity within your school district. It may be challenging to narrow down all the questions or *know* where to start. Risk assessments are critical to understanding your cybersecurity posture. According to the Cybersecurity & Infrastructure Security Agency (*CISA.gov*[2]) – "Cybersecurity (cyber) risk assessments assist public safety organizations in understanding the cyber risks to their operations (e.g., mission, functions, critical service, image, reputation), organizational assets, and individuals." Based on best practices, expert recommendations, district identified priorities, and the agency's own approach to cybersecurity, the MDE has broken down many areas to consider within the context of your district's cybersecurity planning and your overall cybersecurity posture.

There are four sections to this chapter: External Audits, Internal Audits, Reporting and Planning.

A. External Audits: How to measure risks

Understanding the cyber risks to your operational data is the main reason to conduct risk assessments. External audits and risk assessments conducted at least annually are one of the most important strategies for identifying risks to your data. Third party providers offering external audits and risk assessment services serve as objective examinations of your organization's cybersecurity profile and offer the opportunity to "see what the hackers see". The findings from external audits will inform your cybersecurity mitigation roadmap and help you prioritize issues such as changes to your environment, emerging threats, end of support lifecycle for key systems, new strategies, and best practices.

While third party assessments may use many methodologies, most standard assessments encapsulate the following areas:

1. Network Architecture
2. External Penetration
3. Internal Penetration
4. Operating Systems Assessment
5. Specific Host Assessment – IOT, Camera systems, Door control, etc.
6. Risk Prioritization
7. Recommendations on remediations.

A good third-party assessment will provide an executive summary of findings as well as an in-depth explanation of those findings for staff use in the remediation process.

Best Practice –

[1] Chapter 1. "To Know" is an excerpt from the MDE's 2023 K12 Security Advisory Guidance for Improving Cyber Security in Mississippi School Districts. For the full guidance, please visit Information Security and Data Privacy section of the MDE website [*Information Security and Data Privacy | The Mississippi Department of Education (mdek12.org)*].

[2] The Cybersecurity & Infrastructure Security Agency (CISA) [*https://www.cisa.gov/*] is an agency within the US Department of Homeland Security.

At *least once* a year via a third-party organization or vendor that specializes in the service. In concert with continuous monitoring of changes to systems, applications, and user base of your organization compared against the normal operations (*explored further in Section B below*) will give you the most comprehensive understanding of your cybersecurity posture.

Resources –

1. Third Party Assessments – Mississippi Department of Information Technology Services provides an easy procurement process for Security Assessment Services through *RFP3735*. Individual RFPs can be conducted so long as they conform to state law and regulations.
2. CISA's *Cyber Hygiene Scanning Service*
    a. Resources for helping with assessments
    b. Free to school districts
3. Mississippi State University and the "Virtual Institutes for Cyber and Electromagnetic Spectrum Research and Employ" (*VICEROY*) Program
    a. Resources for helping with assessments
    b. Part of a DOD grant
    c. Free to school districts
    d. *Cyber Assessment Interest Form*

B. Internal Audits: How to Protect Users and Devices

A second important strategy for finding the risks to your data is conducting a broad and ongoing internal self-assessment. Separating your user and device auditing from assessments of IT systems allows for a deeper understanding what directly affects the use and conditions of our systems on a day-to-day basis. Self-assessments allow you to discover vulnerabilities that can be addressed immediately.

Policies, procedures, and standard operating procedures (SOPs) should always be in place to make sure that users know their role, what tools to use, and how to properly use systems. Audits verify this knowledge and capability. Achieving a mature level of knowing requires a commitment to define, implement, manage, measure and improve processes that reach all devices and all members of your organization.

Two commonly overlooked elements of your security profile which will be highlighted in an internal audit are:

- **Patching:** Internal audits let you know what your systems are lacking in patching and configuration updates as well as where your endpoints are in the lifecycle. Patches and updates to applications, operating systems, and network devices automatically enable important services and "new features." After a good round of updates and reboots, it is a great idea to scan endpoints for vulnerabilities using tools that give your team the opportunity to verify that patches and configurations take hold. Such tools will notify you of the hosts that are still vulnerable due to "Common Vulnerabilities and Exposures" (CVE).
- **User Browsing Activity:** An internal audit can reveal vulnerabilities based on user browsing activity that can be exploited by threat actors. Threat actors can combine user contact information exposed on your public-facing websites with data on the type of sites the user frequently accesses. Once a threat actor has completed enough reconnaissance, they can send a

phishing email tailored to the user's personal interests. This elevated targeted phishing is also known as "spear phishing." Browsing activity data allows you to tailor acceptable use policies and user training to reduce risks to your organization.

Common Auditing Tools

When it comes to auditing computer user accounts, there are various resources and tools available that can help you with the process. The following list includes categories of **commonly** used tools and resources for auditing computer user accounts:

- Active Directory (AD) Tools: If you are working in a Windows environment, Active Directory is a powerful tool for managing user accounts. It provides various built-in auditing capabilities that allow you to track user account changes, logon events, and other relevant activities.
- G-Suite Environment Tools: If you are working in a Google environment, Enable audit logging in your Google Admin console. This allows you to track and record various activities within your G Suite environment, including user login events, file access, settings changes, and more.
- Security Information and Event Management (SIEM) Systems: SIEM systems aggregate and analyze log data from various sources, including user account activity logs. They can help you monitor and detect suspicious or unauthorized activities related to user accounts.
- User Activity Monitoring Tools: These tools are designed specifically for monitoring user activities on computer systems. They can provide detailed insights into user account usage, including logon times, application usage, file access, and more.
- Password Auditing Tools: Passwords are a critical aspect of user account security. Password auditing tools can assess the strength and security of user passwords, identify weak or easily guessable passwords, and enforce password policies.
- Privileged Access Management (PAM) Solutions: PAM solutions help manage and monitor privileged user accounts, which have elevated access rights. They offer features like session monitoring, access controls, and activity logging to ensure accountability and security.
- Vulnerability Assessment Tools: While not solely focused on user account auditing, vulnerability assessment tools can identify weaknesses and vulnerabilities in systems, including user account-related vulnerabilities.
- Log Management and Analysis Tools: Comprehensive log management and analysis tools, enable centralized collection, storage, and analysis of log data. These tools can help you review and analyze user account-related log entries for auditing purposes.

Best Practices

Remember to ensure that any auditing activities you undertake comply with legal and ethical requirements, including privacy regulations and internal policies. Consider working with your internal counsel to create policies and procedures that ensure your staff is aware that they are being monitored while using school district equipment.

Resources

1. CISA's Cybersecurity Evaluation Tool -- School districts seeking assistance in self-assessments can utilize the Cybersecurity Evaluation Tool to provide "a systematic and repeatable approach for assessing the security posture of their cyber systems and networks."
2. Web browsing activity monitoring

3. Password resiliency – move to MFA (Multifactor Authentication)
4. Self-Assessment - CISA Cybersecurity Evaluation Tool CSET® Demonstration Webinar V4 - YouTube
5. Infosec – CBK – for cybersecurity concepts

C. Reporting: How to report results of external and internal audit findings

Cybersecurity audits assess an organization's security controls, policies, and procedures to identify vulnerabilities and ensure compliance with FERPA, CIPA standards and privacy regulations. The report generated after a cybersecurity audit provides an overview of the audit findings, recommendations, and any identified risks.

The formal report you receive from an application, or the third-party auditor may not come in a format that is appropriate for all audiences. Some questions you may want to ask about communicating the results include:

- Which stakeholders need to be made aware of the reported information?
- What level of understanding do different stakeholder(s) have when it comes to technology?
- Is there information included in the report which should not be divulged to certain stakeholders based on their roles?
- How can you adapt the important takeaways from your report(s) and make them understandable and actionable for different stakeholders?

Best Practices

Prior to receiving the results of your audits, identify all stakeholder groups in your district who may need or desire to be kept aware of the status of your security profile. Make note of each group's level of understanding of technology issues and whether they should be privy to any sensitive information contained in reports.

Resources

1. *How to Talk to Stakeholders about Cybersecurity*
2. *Align security guidelines with all current policies and procedures*.

D. Cyber Security Planning

The audit, mitigation, verification, cycle allows you "To Know" where you are in the cybersecurity environment within the context of a technology policy and process framework. With a verified data backup solution and the ability to be insured, your district will be in a much better position to respond to incidents. This continuous feedback also gives you better insight into the actual workings of the underlying technology which with upgrades and updates are a consistently moving target. Knowing where you are now in the cybersecurity loop will allow for a more confident incident response when an event does occur.

Best Practices

Discussions about cyber security auditing, reporting and planning in your district should include important stakeholders including individuals and groups responsible for finance and operations, building maintenance, administration, and policy development and approval. Stakeholder groups may use this

document to guide the development of their cybersecurity plans. The plans also should be well informed by district self-assessment.

Resources

1. *Deep dive into cybersecurity planning from the FCC*
2. *Cybersecurity Considerations for K1-12 Schools and School Districts from US Department of Education*