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 2. "To Do"[1]: The Mitigation Feedback Loop

Cybersecurity remediation in a school district's information technology profile includes a continuous and systematic approach to identifying, assessing, and mitigating vulnerabilities and threats. This process is vital to enhance the district's cybersecurity posture and protect sensitive data, student information, and critical infrastructure. The loopback processes created from this will continue to "sharpen the saw". This document offers a methodology in which you can develop your own cybersecurity plans to include this process.

Chapter 2 includes four sections:

A. Identification, Reconciliation and Comparison

B. Assessment of Gaps and Vulnerabilities

C. Mitigation Planning

D. Mitigation Implementation, Verification and Change Control

A. Identification, Reconciliation and Comparison

After a risk assessment (see Chapter 1: To Know), a comprehensive inventory of all IT assets, systems, and applications used within the school district should be compared to the assessment results. In this process the district should identify which devices are no longer supported by the manufacturer and in consideration for elimination. Networking and server hardware terminology refers to this as End of Life (EOL) for their assets. This includes any updates to the code or software that runs on the hardware. End of Support (EOS) is commonly found with operating systems or applications that have been supported beyond a certain date. Usually, this date is set for a period after a newer version has been released.

Best Practices –

Identifying these issues in hardware and software is a first step. Since there is likely to be no mitigation path for EOL and EOS assets, the best approach is to eliminate their use. The district should identify the functions those systems support and either replace them with an updated system or change to another process. This is especially important when dealing with previously missing or lost devices. These devices may reappear with various older software/hardware issues which can pose a significant vulnerability. Automation in network hardware/software management can alert staff when out of date device become present either wired or wirelessly.

- Prioritize Assets: Categorize assets based on their criticality and potential impact on the school district if compromised. This helps in prioritizing remediation efforts.
- Prioritize Vulnerabilities: Categorize the identified vulnerabilities based on their severity and potential impact on the school district's systems and data. This helps in focusing efforts on critical issues first.
- Security Patch Management: Establish a robust process for managing security patches and updates for all software, applications, and operating systems. Regularly update and patch systems to eliminate known vulnerabilities.

[1] Chapter 2. "To Do" 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)*].

- Create a Mitigation Plan: Develop a comprehensive mitigation plan that outlines specific actions, timelines, and responsible parties for addressing each identified vulnerability.
- Implement Security Controls: Deploy appropriate security controls, such as firewalls, antivirus software, intrusion detection/prevention systems (IDS/IPS), encryption, multi-factor authentication (MFA), and access controls, to safeguard systems and data.
- Continuous Monitoring and Incident Detection: Employ continuous monitoring tools and techniques to detect suspicious activities, potential security breaches, and abnormal behaviors in real-time.
- Continuous Improvement and Feedback Loop: Review the results of vulnerability assessments, penetration tests, and incident responses regularly. Use this feedback to refine and improve the overall cybersecurity strategy continually.
- Stay Updated: Continuously monitor emerging cybersecurity threats, industry best practices, and new technologies to adapt the remediation process accordingly.

Resources –

- ***The National Security Agency's (NSA) Top Ten Cybersecurity Mitigation Strategies*** (PDF) to counter techniques used by threat actors
- ***2021 Top Routinely Exploited Vulnerabilities***, a Cybersecurity Advisory from the US Cybersecurity & Infrastructure Security Agency (CISA)
- ***2022 CWE Top 25 Most Dangerous Software Weaknesses*** from Common Weakness Enumeration (CWE), a cybersecurity community-developed list of common software and hardware weaknesses with security ramifications
- ***End-of-life (EOL) Date Web Site***, a project of GitHub to track various end-of-Life dates and support lifecycles for various products.

B. Assessment of Gaps and Vulnerabilities

Assessments should not be viewed as one-time events, districts should always be running some type of assessment. In the military, ongoing assessment is known as "situational awareness." Knowing where your assets (elements) are, the capabilities of those assets (abilities), where/how they are being used (environment), and the timelines that effect vulnerabilities of those assets will give you the current status of your cybersecurity profile. Understanding the results of a third-party assessment will set the baseline from which you can build a process of continuous improvement. As new assets come online and older assets reach EOL/EOS, new vulnerabilities discovered and announced each day must be constantly tracked.

Best Practices –

- Adopt Security Standards and Frameworks: Implement widely recognized cybersecurity standards and frameworks, such as NIST Cybersecurity Framework or CIS Controls, to guide the remediation process and ensure compliance.
- Reconcile Your Inventory: Export all necessary information about physical assets still on the inventory from the accounting system. This will help you with the validation of known, trusted devices and the manufacturer's state of support for those devices.

- Network Infrastructure Updates: Validate that all devices suppporting your network infrastructure are up to date, and configurations are secure from manipulation. Updating admin access controls, wireless password access, and configuration of segmented networks isolate the potential for outages caused by threat actors.
- Penetration Testing: Conduct periodic internal penetration testing exercises to simulate cyber-attacks and identify vulnerabilities that might not be detected by automated tools.
- Third-Party Risk Management: Assess the cybersecurity posture of third-party vendors and service providers to ensure they meet the same security standards as the school district.

Resources –

- ***CIS Control 7: Continuous Vulnerability Management***, recommendations from the Center for Internet Security (CIS).
- ***The National Vulnerability Database***, a repository of standards-based vulnerability management data from the National Institute of Standards and Technology (NIST)
- ***How to Assess a Vendor's Data Security***, guidance from the Electronic Frontier Foundation (EFF)

C. Mitigation Planning: Vulnerabilities and Threats

After creating a comprehensive inventory of all the software and systems used by your organization and categorizing them based on criticality and potential impact on business operations, you move to the mitigation steps. Mitigating vulnerabilities and the threats they pose is a constant battle. Automated patch deployment can significantly reduce the patching window and ensure that critical updates are applied consistently and without delays. A best practice for patch management is to implement a well-structured and systematic approach to ensure that all network devices, software, operating systems, and applications are promptly and securely updated with the latest patches.

Best Practices –

- Patch Monitoring and Notification: Stay informed about the latest security patches released by software vendors and security advisories. Subscribe to official mailing lists, security forums, and news sources to receive timely notifications of new patches.
- Test Patches in a Controlled Environment: Before deploying patches across the entire organization, test them in a controlled environment, such as a test network or a limited set of systems. This testing phase ensures that patches don't introduce new compatibility issues or cause disruptions.
- Establish Patching Policy and Schedule: Develop a clear patching policy that outlines the frequency of patch updates, the roles and responsibilities of involved personnel, and the expected timeline for deploying patches. Create a predictable patching schedule to minimize disruptions and make it easier for IT teams to plan their activities.
- Fallback and Rollback Plan: Despite testing, unexpected issues may arise after patch deployment. Develop a fallback and rollback plan to quickly revert to the previous state if a patch causes problems that cannot be immediately resolved.
- Maintain Documentation: Keep thorough documentation of the patch management process, including the patches deployed, dates, and any issues encountered. Documentation helps with audits, compliance requirements, and future reference.

- Continuous Improvement: Regularly evaluate and improve your patch management process based on lessons learned from incidents, feedback from users, and changes in your organization's IT landscape. Continuously updating the process ensures it remains effective against evolving threats.
- Monitor and Verify Patch Deployment: After patches are deployed, monitor the affected systems to ensure that the updates were successful and didn't cause any adverse effects. Verification can be done through various monitoring tools and by seeking feedback from users.

Resources –

- ***6 steps for a solid patch management process***, guidance from CSO Online
- ***Best Vulnerability Management Tools Reviews 2023***, vulnerability assessment reviews and ratings from Gartner Peer Insights
- ***Vulnerability Management | A Complete Guide and Best Practices***, an explanation of vulnerability management and guide to impmenting a vulnerability management process from HackerOne
- ***Vulnerability Management Resources***, a post from SANS Institute including a collection of no-cost resources focused on vulnerability management (news, webcasts, surveys, live streams, blogs, etc.)

D. Mitigation Implementation, Verification and Change Control

With any updates to systems, awareness of the effects of the updates must be considered. What is the impact of your updates on the devices and systems your district users depend on? Desktops and laptops depend on network switches to be functional, servers are dependent on core switches, and almost everything in your infrastructure is dependent on the firewall for internet access. When creating a change plan for mitigation of vulnerabilities, you should start with the least impacting devices. This gives you and your staff time to build confidence that patches, configuration changes, and removal of devices or software that is no longer supported will not adversely affect the environment because of dependencies.

Best Practices –

- Create a detailed action plan for implementing the chosen mitigation strategies. This plan should outline specific tasks, responsibilities, timelines, and resources required for each mitigation action.
- Prioritize mitigation actions based on the potential impact of the risks they address. Address high-priority risks first but ensure that all identified risks are eventually covered.
- Begin implementing the chosen mitigation measures according to the action plan. After implementation, conduct thorough testing and verification to ensure that the mitigation measures are effective and functioning as intended. This could involve security testing, vulnerability scanning, and simulations of potential attacks.
- Maintain detailed documentation of the entire mitigation plan. Document risk assessments, mitigation strategies, action plans, testing results, and any changes made to the IT environment.
- Continuously monitor the effectiveness of the implemented mitigation measures. Regularly review and update the mitigation plan to address evolving threats, changes in the IT environment, and new vulnerabilities.

- Periodically review and audit the cybersecurity mitigation plan to assess its effectiveness and make necessary updates. This ensures that the plan remains aligned with the changing threat landscape and organizational needs.

Resources –

- ***CRR Supplemental Resource Guide, Volume 3: Configuration and Change Management*** (PDF), from the guide developed by the Department of Homeland Security's (DHS) Cyber Security Evaluation Program (CSEP) to help organizations implement practices identified as considerations for improvement during a Cyber Resilience Review (CRR)
- ***The National Security Agency's (NSA) Top Ten Cybersecurity Mitigation Strategies*** (PDF) to counter techniques used by threat actors (also referenced in Part A)
- ***Layer 2 Attacks and their Mitigation*** (PDF), slide deck of a security bootcamp presentation by staff at Cisco

Chapter 2 Wrap-Up

The mitigation feedback loop process in cybersecurity involves systematically identifying vulnerabilities, assessing their risk, planning your mitigation strategy, and implementing appropriate mitigations. This iterative approach helps you to adapt to emerging threats, minimize risks, and safeguard digital assets.

For an district's security plan to be effective, it must reflect such a continuous feedback loop. By continuously repeating the cycle of identifying, assessing, and mitigating vulnerabilities, your security plans can adapt to changing threat landscapes, emerging attack techniques, and evolving technologies. This process allows you to refine security plans and stay ahead of potential threats.

Throughout the entire process, documentation and communication are crucial. Detailed records of identified vulnerabilities, assessment results, mitigation actions taken, and the outcomes of those actions should be maintained within the security plan. Effective communication ensures that relevant stakeholders are aware of the security status and are aligned on the necessary actions.