Mississippi Cyber Security Review Board
September 5, 2024

Securing Mississippi

Cybersecurity Best Practices

Table of Contents

Executive Summary ....

As a result of Senate Bill 2698, the Mississippi Cyber Security Review Board (CSRB) shall be responsible for creating a whole-of-state strategy to address the threats to the state of Mississippi. This is a critical process for achieving the desired results of a stronger cyber security posture. The responsibilities of the board include creating a system for reporting cybersecurity attacks within the state, researching and implementing best practices to mitigate cybersecurity risks, and connecting individuals and entities with federal and industry partners.

Inconsistent cybersecurity practices and investments across different sectors create exploitable gaps, increasing the risk of serious disruptions. The CSRB recognizes this gap and has compiled a list of initial best practices to support good cyber hygiene. Properly implemented, these recommendations will have a high impact on improving the overall cybersecurity posture of Mississippi's key assets, identified as: K12 schools, local government, state government, and critical infrastructure. The CSRB's best practices are applicable across all sectors by focusing on the baseline security practices creating protections for common adversary tactics, techniques, and procedures (TTPs).

This list is a minimum set of cybersecurity best practices that should be implemented across all digital infrastructure. These best practices directly support the Cybersecurity and Infrastructure Security Agency (CISA) and the State of Mississippi's efforts to address common cybersecurity protections. The CSRB's collection of best practices specifically coordinates with the standards specified in the Mississippi Department of Information Technology Services (ITS) State of Mississippi Enterprise Security Policy, and CISA's Cross-Sector Cybersecurity Performance Goals (CPGs) to create the baseline.[i] Both agencies have created a practical, risk-based approach that helps organizations build a robust cybersecurity posture tailored to their specific needs and challenges. This collection will function as a comprehensive reference for any Mississippi-based digital infrastructure with critical importance to state and local government entities. By strengthening the state's understanding and capacity to handle cyber risks, the CSRB will bolster its collective defense, protect sensitive data, and ensure the continued safety and trust of Mississippians.

Introduction...

To achieve a comprehensive whole-of-state cybersecurity approach, the CSRB is introducing a collection of best practices based on the established frameworks of the ITS Enterprise Security Policy and CISA CPGs. By combining these structured guidelines with specific performance targets, this integrated strategy provides a robust foundation for enhancing cybersecurity across all sectors in Mississippi. Both frameworks have proven effective in improving cybersecurity for organizations of various sizes and sectors, regardless of their existing security maturity.

The CSRB recognizes that Mississippi organizations have unique risks, tolerances, objectives, and goals. Therefore, the approach to managing risks and implementing cybersecurity measures should be tailored to individual needs. The CISA CPGs address this requirement by providing broad, clearly defined goals that can be communicated across different sectors.

The CSRB's collection of best practices focuses on five key categories:

- **Identify:** Understanding and managing cybersecurity risks.
- **Protect:** Implementing safeguards to prevent or mitigate threats.
- **Detect:** Identifying security events for timely responses.
- **Respond:** Effectively managing and mitigating the impact of incidents.
- **Recover:** Restoring and improving capabilities after an incident.

By organizing these functions into separate categories, the CSRB aims to create a balanced and integrated cybersecurity strategy that addresses all critical areas for a successful whole-of-state approach.

Cyber Hygiene ....

Despite heightened awareness of cyberattacks, numerous organizations remain vulnerable due to a lack of fundamental cybersecurity measures. Small organizations, often constrained by limited resources, can face challenges in implementing robust security practices. However, the adoption of basic cyber hygiene principles can significantly mitigate these risks by establishing a baseline for the implementation of additional cybersecurity controls that specifically address the risk to the individual organization. Cyber hygiene, a foundational aspect of cybersecurity, encompasses essential practices and protocols for safeguarding infrastructure from security threats.

While this is not the exhaustive list of all cybersecurity activities that an organization should implement, organizations of any size should ensure that the following cybersecurity controls have been implemented to protect against the most well-known cyber-attacks and provide a strong return on investment:

- **Multi-Factor Authentication (MFA):** Significantly reduces the risk of unauthorized access even if passwords are compromised, as it blocks most account-based attacks.[ii]
- **Security Awareness Training:** Phishing attacks are one of the most dangerous types of attacks to even the most secure environments because they prey on human error. Proper training ensures that employees understand the importance of security protocols, can identify suspicious activities, and adhere to best practices for protecting sensitive information.[iii]
- **Endpoint Detection and Response (EDR):** Monitoring endpoints for suspicious activities enables rapid detection and response to threats like malware, ransomware, and other malicious behaviors that can minimize the impact of attacks.
- **Patch Management:** Many cyber-attacks exploit known vulnerabilities in software, so regularly updating and patching systems closes these security gaps.
- **Network Segmentation:** By segmenting networks, organizations can limit the spread of malware and reduce the potential damage from an attack by limiting the attack surface and protecting critical assets.
- **Email Filtering and Protection:** Due to the prevalence of email-based attacks, implementing robust email filtering can prevent many threats from reaching users and the ability to stop threats before they enter the network.

- **Least Privilege Principle:** Users and systems should only have the minimum level of access necessary to perform their functions. This reduces the risk of insider threats and limits the impact of compromised accounts.

By adopting these essential security measures, organizations can significantly reduce their risk of falling victim to cyberattacks. These controls provide a solid foundation for combatting the escalating number of cyber incidents by addressing many common attack vectors and vulnerabilities. The CSRB advocates for a proactive approach to cybersecurity, emphasizing the importance of implementing these practices to safeguard sensitive information, protect organizational assets, and maintain operational integrity.

Best Practices ....

The integration of CISA CPGs combined with the standards specified in the ITS Enterprise Security Policy, presents a comprehensive and coherent collection of best practices designed to fortify Mississippi's digital infrastructure.[iv] Combining these frameworks ensures that the CSRB's collection of best practices aligns with national standards and state-specific requirements.

- Cybersecurity Infrastructure and Security Agency Cross-Sector Cybersecurity Performance Goals (CISA CPGs): CISA_CPG_REPORT_v1.0.1_FINAL.pdf
- Mississippi Department of Information Technology Services (ITS) State of Mississippi Enterprise Security Policy: 10-1-2013 ESP.pdf (ms.gov)

The following collection of best practices will help strengthen Mississippi's overall digital security posture and resilience:

Identify:

1. **Maintain a comprehensive asset inventory:** Regularly update a detailed list of all organizational devices with internet addresses, including those used for operational technology (OT).
2. **Designate a cybersecurity leader:** Assign a specific role responsible for overseeing and implementing cybersecurity strategies.
3. **Appoint an OT cybersecurity specialist:** Assign a dedicated role to handle the unique security needs of operational technology systems.
4. **Foster collaboration:** Organize at least one annual event to strengthen communication and cooperation between IT and OT security teams.
5. **Address vulnerabilities promptly:** Patch or mitigate known vulnerabilities in internet-facing systems within a reasonable timeframe, prioritizing critical assets first.
6. **Conduct regular security assessments:** Engage third-party experts to evaluate the effectiveness of cybersecurity defenses. Conduct both announced and unannounced exercises to test the organization's ability to detect and respond to breaches.
7. **Require vendor transparency**: Ensure that vendors and service providers notify the organization of any security vulnerabilities or incidents.
8. **Prioritize cybersecurity in procurement:** Incorporate cybersecurity requirements into vendor selection processes to choose the most secure options.

Protect:

1. **Change default passwords:** Implement a policy requiring the modification of default passwords for all devices. If this is not feasible, implement alternative security measures and monitor for suspicious activity. [v]
2. **Enforce strong password policies:** Establish a policy mandating long, complex passwords for all accounts.
3. **Use unique credentials:** Prohibit the reuse of passwords across different accounts.
4. **Implement offboarding procedures:** Revoke access and disable accounts for departing employees.
5. **Limit administrative privileges:** Restrict administrator privileges to essential tasks and require separate accounts for general use.
6. **Secure network access:** Restrict network access to OT systems and require intermediary devices for communication.
7. **Monitor login attempts:** Track unsuccessful login attempts and alert security teams to suspicious activity.
8. **Utilize multi-factor authentication (MFA):** Implement MFA for all accounts, prioritizing high-risk accounts.
9. **Provide cybersecurity training:** Conduct annual training sessions for all employees to raise awareness and improve security practices.
10. **Offer specialized OT training:** Provide OT-specific training to personnel responsible for maintaining and securing operational technology systems.
11. **Encrypt data in transit:** Use secure protocols like SSL/TLS to protect data during transmission.
12. **Safeguard sensitive data:** Store sensitive data securely and restrict access to authorized users.
13. **Protect email communications:** Enable STARTTLS, SPF, DKIM, and DMARC to prevent email-based attacks.
14. **Disable macros:** Disable macros by default and require explicit authorization for their use.
15. **Document asset configurations:** Maintain accurate records of critical asset configurations to facilitate vulnerability management.
16. **Document network topology:** Keep detailed documentation of network infrastructure.
17. **Implement change management:** Establish a process for reviewing and approving changes to hardware, firmware, or software.
18. **Regularly backup systems:** Create backups of critical systems and test them periodically.

19. **Develop incident response plans:** Create and practice incident response plans for various threat scenarios.
20. **Monitor and analyze logs:** Collect and analyze logs to detect security incidents.
21. **Securely store logs:** Store logs in a centralized system and restrict access to authorized users.
22. **Prevent unauthorized media:** Implement policies to prevent unauthorized devices from being connected to networks.
23. **Secure internet-facing assets:** Disable unnecessary services and implement protective measures for exposed assets.
24. **Limit OT internet exposure:** Minimize the exposure of OT assets to the internet.

Detect:

1. **Track relevant threats:** Identify and monitor threats specific to your organization's industry and sector.

Respond:

1. **Report incidents:** Establish procedures for reporting cybersecurity incidents to appropriate authorities.
2. **Encourage vulnerability disclosure:** Provide a public channel for security researchers to report vulnerabilities.
3. **Maintain a security.txt file:** Use a security.txt file to provide contact information for security researchers.

Recover:

1. **Develop recovery plans:** Create and practice plans to restore critical systems and data in the event of a cyberattack.
2. **Develop business continuity plans:** Create and practice plans for continued operations during a cyberattack or other business disruption.

Conclusion ....

Organizations with a high level of maturity not only have robust defenses in place but also utilize a proactive approach to identifying and mitigating potential vulnerabilities. It is imperative that Mississippi entities across all sectors strive for a high level of cybersecurity maturity. The CSRB is coordinating comprehensive guidance and practices to address the cybersecurity risks faced by many Mississippi organizations due to limited resources and/or technical expertise. The CSRB places a priority on strengthening Mississippi's cybersecurity posture to ensure a safer environment for its citizens, businesses, and critical infrastructure. The CSRB's collection of best practices is one of the first essential steps for fortifying the state's cybersecurity landscape and safeguarding citizens' data.

By consolidating proven strategies and guidelines, Mississippi can establish a cohesive and resilient defense against emerging cyber threats. These best practices not only enhance individual organizational security but also contribute to a unified approach that elevates the overall cybersecurity posture of the state. As cyber threats become increasingly sophisticated, having a well-defined set of best practices ensures that Mississippi is better equipped to protect sensitive information, maintain public trust, and uphold the integrity of vital systems. Ultimately, investing in and adhering to these best practices is a proactive measure that strengthens the state's ability to counteract cyber risks and secure a safer digital environment for all its citizens.

Endnotes……………………………………………………………………………

[i] Mississippi Department of Information Technology Services Information Security Division State of Mississippi Enterprise Security Policy. 10-1-2013 ESP.pdf (ms.gov); Cybersecurity and Infrastructure Security Agency (CISA) Cross-Sector Cybersecurity Performance Goals (CPGs). Cross-Sector Cybersecurity Performance Goals | CISA

[ii] CISA CPG 2. H: Phishing-Resistant Multi-Factor Authentication (MFA)

[iii] CISA CPG 2. I: Basic Cybersecurity Training; CISA CPG 2. J: OT Cybersecurity Training

[iv] Mississippi Department of Information Technology Services Information Security Division State of Mississippi Enterprise Security Policy. 10-1-2013 ESP.pdf (ms.gov)

[v] Mississippi Department of Information Technology Services Information Security Division State of Mississippi Enterprise Security Policy. Page 16. 10-1-2013 ESP.pdf (ms.gov)