Mississippi Office of the State Auditor
Shad White

Mississippi Government Offices Potentially Putting Taxpayer Data and Privacy At Risk

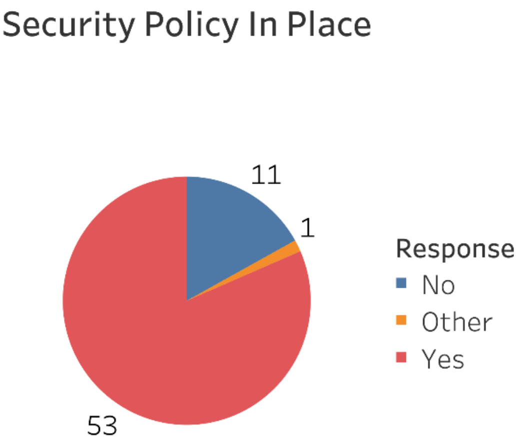
Cyber Security Audit Shows Compliance Failures Around State Government

A Data Services Division Brief

October 1st, 2019

An analysis by the Office of State Auditor Shad White shows that Mississippi government institutions are not in compliance with the Mississippi Enterprise Security Program and industry standard cyber security practices. The Auditor's Office conducted a survey of 125 state agencies, boards, commissions, and universities that connect to the State of Mississippi computer network to verify they are meeting requirements of the State of Mississippi Enterprise Security Program.[1] Compliance with the Program is required by law.

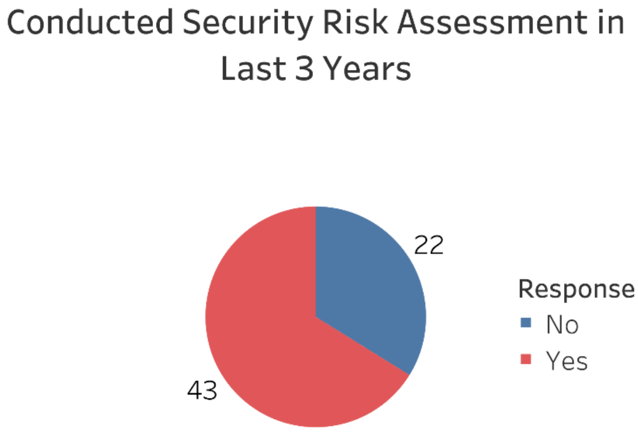
Despite the Auditor's Office being authorized to verify compliance, 54 of the institutions surveyed chose not to respond. Auditing security practices is an essential function of ensuring that taxpayer funds and data remain safe and that agencies are protected from intrusions. Failure to submit to this audit is a failure of duty by the agency and creates increased risk for the State and its citizens.



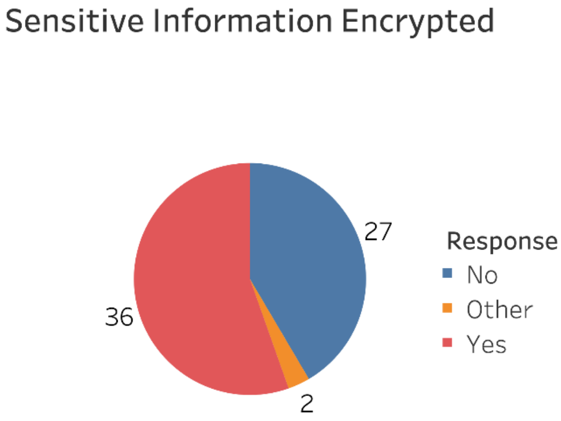
Documenting policies and procedures is one of the most important measures an institution can take to ensure proper cyber security practices. These policies document infrastructure, procedures for mitigating risks and vulnerabilities, procedures for reporting security incidents and responding to them, as well as general policies and acceptable use rules for end users. **Of the 71 agencies who responded to the survey, 11 reported not having a security policy plan or disaster recovery plan in place.**

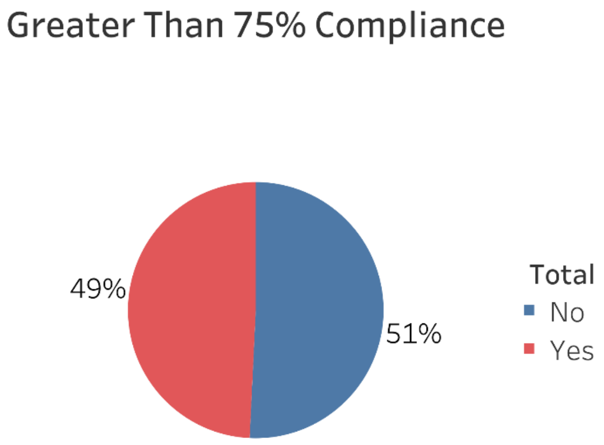
[1] Mississippi Code Ann. 25-53-201

State institutions are required by law to have a third party perform a Security Risk Assessment at least once every three years. A third party assessment is essential for identifying areas of weakness within an institution’s cyber security posture in order to mitigate these risks and prevent future security incidents. **In the survey, 22 agencies indicated they have not had an assessment done, leaving them vulnerable to hacking and out of compliance with state law.**


Conducted Security Risk Assessment in Last 3 Years

The State of Mississippi creates, stores, and maintains a wealth of sensitive information. Health data, tax data, student data, and any number of personally identifiable data are examples of sensitive information. It is critical that sensitive information is encrypted when stored or transmitted. Proper encryption helps prevent unauthorized access of data even in the event of an intrusion. Furthermore, federal guidelines require that certain data be encrypted. **Of all survey respondents, 38% of agencies reported not encrypting sensitive information, thus putting data at high risk.**


Sensitive Information Encrypted



The survey contained 59 questions that related to specific requirements in the Enterprise Security Program. The three results presented here represent only a small portion of the problems that were identified and are used to highlight the issues that exist within cyber security in state government. **Over half of the respondents were less than 75% compliant with the Enterprise Security Program. These numbers do not include the 54 institutions who chose not to respond.**

Conclusion

The State Auditor's office is required under state regulations to monitor compliance with certain cyber security laws and regulations. As a part of its responsibility, auditors surveyed state government agencies, boards, and commissions. The results of the survey described above show that Mississippians' personal data may be at risk. Many state agencies are operating as if they are not required to comply with cyber security laws, and many refused to respond to auditors' questions about their compliance. State government cyber security is a serious issue for Mississippi taxpayers and citizens. Mississippians deserve to know their tax, income, health, or student information that resides on state government servers will not be hacked.

Leaders of agencies need to question their information technology professionals in their office to be sure their agency is compliant. Each agency should also consider ways to go above and beyond to prevent cyber breaches. The Office of the State Auditor (OSA), for instance, partnered with the federal Department of Homeland Security (DHS) and allowed DHS to try to hack OSA computers to test for vulnerabilities. OSA employees are also required to go through training to spot phishing attempts and learn best practices for preventing security incidents. Finally, state leaders should continue to collaborate and share cyber security best practices both between state agencies and with local governments.

*Note that the total count of responses in the graphs is not representative of the total number of institutions that responded to the survey. Some institutions did not answer every survey question.