Nicole Galloway, CPA
Missouri State Auditor

CITIZENS SUMMARY

Summary of Audit Findings in Cyber Aware School Audits

Background

The Cyber Aware School Audits were designed to assess the effectiveness of privacy and security controls with a focus on identifying practices that improve the security of information school districts have on students and their families. This report summarizes the cybersecurity risks identified from these audits.

Data Governance

The audits found that in many cases a comprehensive data governance program was not established or completed. Data governance is an organizational approach to data and information management that is formalized as a set of policies and procedures encompassing the full life cycle of data, from acquisition to use to disposal. It includes establishing policies, procedures, and standards regarding data security and privacy protection, data access, and data sharing. Without a comprehensive data governance program, there is less assurance the data management and protection procedures in place are effective in reducing data privacy and security risks due to unauthorized access or misuse of data.

User Accounts

The audits found controls for creating and maintaining user accounts for accessing system resources were not fully established. For example, policies and procedures for disabling or removing user accounts timely after a user ended employment were not documented, or required additional steps and policies and procedures for requesting, establishing, and maintaining user access to data and other system resources were not formally documented. Proactive monitoring for user accounts not accessed or used for a specified period of time was not performed. Periodic reviews of user access to data to ensure access remained appropriate and aligned with job duties were not performed. Certain staff shared user accounts and passwords, which meant actions taken cannot be traced back to a specific user. Without appropriate account access policies and procedures, users may have inappropriate or unauthorized access, which can provide opportunities for misuse or inappropriate disclosure of sensitive data.

Security Controls

In many cases the audits found not all necessary security controls were implemented, leaving district technology assets, including personally identifiable information, at risk of inappropriate access, use, and disclosure. For example, specific personnel were not formally appointed to serve as security administrator or formally assigned responsibility for creating, implementing, and maintaining security policies and procedures. Network passwords were not required to be periodically changed and controls to enforce the use of strong passwords were not required. Policies and procedures regarding user access to systems and data, including the use of logon banners and controls to manage concurrent access to systems, were not fully established. Policies and procedures to identify the types of security events to be logged and monitored were not formally documented or the documented policies needed to be enhanced. Physical security controls were not fully established to ensure protection of technology resources. Policies and procedures for certain security controls were not documented. Without a formal designation of staff responsible for security administration, and without documented and approved policies and

	procedures, management may not have assurance that control activities are appropriate and properly applied.
Incident Response and Continuity Planning	The audits found additional measures were necessary to protect data in the event of a breach or other disruptive incident. Policies and procedures for responding to security incidents were not formally documented, a comprehensive data breach response policy was not established, or a complete continuity plan was not documented and formally tested. Without prompt and appropriate responses to security incidents, violations could continue to occur and cause damage to an organization's resources. Without a comprehensive data breach response policy, management may not be sufficiently equipped to respond quickly and effectively in the event of a breach, increasing the risk of potential harm to affected individuals.
Security Awareness Program	The audits found a lack of a formal security and privacy awareness training program. As education organizations implement more powerful information systems and become more reliant on electronic data, proactive security awareness programs become a priority. Uninformed users are a major threat to data security in education organizations. Without adequate training, users may not understand system security risks and their role in implementing related policies and controls to mitigate those risks.
Vendor Controls	The audits found controls for monitoring vendors and contracts were not fully established. Processes did not exist to ensure software acquired or outsourced from information technology vendors complied with data security principles. In some cases, a written contract was not established with the vendor of a critical district system or the contract did not fully define expectations over securing and accessing district data. Without an effective process for monitoring and managing risk of software acquisition or outsourcing, and without a written contract that fully defines data security expectations, districts have less assurance that services meet current and future data privacy and security needs.

Because of the nature of this report, no rating has been provided.

All reports are available on our Web site: auditor.mo.gov