Office of Missouri State Auditor

Nicole Galloway, CPA

Summary of Audit Findings
Cyber Aware School Audits

Report No. 2016-112
October 2016

auditor.mo.gov

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

Summary of Audit Findings
Cyber Aware School Audits
Table of Contents

State Auditor's Report 2

Introduction

Background 3

Audit Issues

1. Data Governance 7
2. User Accounts 8
3. Security Controls 9
4. Incident Response and Continuity Planning 13
5. Security Awareness Program 15
6. Vendor Controls 15

Appendix

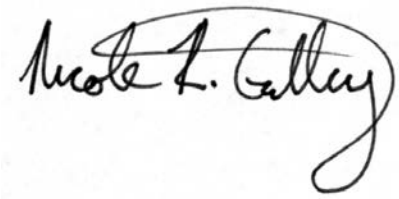
Audit Reports 17

NICOLE GALLOWAY, CPA
Missouri State Auditor

Honorable Jeremiah W. (Jay) Nixon, Governor
and
Members of the General Assembly
and
Dr. Margie Vandeven, Commissioner
Department of Elementary and Secondary Education
Jefferson City, Missouri

This report was compiled using the five audits completed between March and September 2016 as part of the State Auditor's Cyber Aware School Audits Initiative. That initiative focused on evaluating the effectiveness of data governance programs, including identifying cybersecurity safeguards and privacy controls that can help schools improve the security of student data. The objective of this report is to summarize the common cybersecurity, privacy, and security control issues and recommendations discussed in those audits to raise awareness and assist other school districts in identifying strengths and areas where improvements can be made in their data governance programs.

The recommendations address a variety of topics including data governance, user accounts, security controls, incident response and continuity planning, security awareness, and vendor monitoring. The Appendix lists the five audit reports issued. The issues and recommendations presented in this report may not have been applicable to each of the five districts and each district may have had varying levels of controls established for each issue. As a result, refer to each district's audit report for findings and recommendations applicable to that district.



Nicole R. Galloway, CPA
State Auditor

The following auditors participated in the preparation of this report:

Deputy State Auditor:	Keriann Wright, MBA, CPA
Director of Audits:	Douglas J. Porting, CPA, CFE
Audit Manager:	Jeffrey Thelen, CPA, CISA

Summary of Audit Findings
Cyber Aware School Audits
Introduction

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.

Districts use a student information system (SIS) to maintain student data and to track and monitor academic progress. The SIS maintains private and confidential data, such as assessment test scores and other sensitive data. Districts upload various student data maintained in the SIS to the Department of Elementary and Secondary Education (DESE), Missouri Student Information System (MOSIS) Data Collection component periodically throughout the year. The MOSIS Data Collection component is used to collect student-level data from school districts for processing and reporting. Data submitted by districts include elements such as enrollment and attendance, demographics, performance information, and college and career data used for evaluating the success and achievements of students. Districts also use a financial accounting system and a network management system for administering user access to various district resources. Other systems and applications are used for administrative functions and to enhance student productivity and classroom collaboration.

Cyber threats continue to emerge and evolve

As connectivity of business activity increases and organizations become increasingly dependent on technology, including computerized systems and electronic data, no school district is exempt from cyber threats, vulnerabilities, and privacy exposures. As a result, it is important to view information security and privacy as a business issue rather than strictly an information technology issue. Security threats, vulnerabilities, and privacy exposures challenge every organization, creating data protection and privacy risks that must be understood, addressed, and managed.

In the 2015 High-Risk Series[1] update, the Government Accountability Office (GAO) expanded the scope of the information security high-risk area to include protecting the privacy of personally identifiable information (PII).[2] The GAO expanded this risk area due to the challenges of ensuring

[1] Report GAO-15-290, Report to Congressional Committees, High-Risk Series An Update, February 2015, is available at <http://www.gao.gov/assets/670/668415.pdf>.

[2] According to the Family Educational Rights and Privacy Act (FERPA), personally identifiable information (PII) includes, but is not limited to (a) the student's name; (b) the name of the student's parent or other family members; (c) the address of the student or student's family; (d) a personal identifier, such as the student's social security number, student number, or biometric record; (e) other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name; and (f) other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student.

the privacy of PII created by advances in technology. Technology advances, such as lower data storage costs and increasing interconnectivity, have allowed both government and private sector agencies to collect and process extensive amounts of PII more effectively. Risks to PII can originate from unintentional and intentional threats. These risks include insider threats from careless, disgruntled, or improperly trained employees and contractors; the ease of obtaining and using hacking tools; and the emergence of more destructive attacks and data thefts.

Technology advances, combined with the increasing sophistication of individuals or groups with malicious intent, have increased the risk of PII being compromised and exposed. Correspondingly, the number of reported security incidents involving PII in both the private and public sectors has increased dramatically in recent years. At the same time, school districts are increasingly reliant on technology and information sharing to interact with students and parents and to deliver essential educational services. As a result, the need to protect information, including PII, against cyber threats is increasingly important.

Data governance

According to the U.S. Department of Education, Privacy Technical Assistance Center (PTAC),[3] 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 inventories, content and records management, data quality control, data access, and data sharing and dissemination.

Security and privacy controls

According to accepted standards, security controls are the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of a system and its information. Confidentiality refers to preserving authorized restrictions on information access and disclosure, including the means for protecting personal privacy and proprietary information. Integrity relates to guarding against improper information modification or destruction, and availability ensures timely and reliable access to and use of information. Effective privacy controls depend on the safeguards employed within the information system that is processing, storing, and transmitting PII and the environment in which the system operates. Organizations cannot have effective privacy without a basic foundation of information security.

[3] U.S. Department of Education, Privacy Technical Assistance Center, Data Governance Checklist, is available at <http://ptac.ed.gov/sites/default/files/Data%20Governance%20Checklist%20%281%29.pdf>.

Laws and regulations

Various federal and state laws and regulations pertain to the protection of sensitive student data, including the Family Educational Rights and Privacy Act (FERPA), the Individuals with Disabilities Education Act (IDEA), and the Protection of Pupil Rights Amendment (PPRA). Additionally, Section 161.096, RSMo, requires the State Board of Education to promulgate a rule regarding "student data accessibility, transparency, and accountability."[4]

Standards and best practices

We based our evaluation of the effectiveness of the school districts' data governance programs on accepted state, federal, and international standards; policies and procedures; and best practices related to information technology security and privacy controls from the following sources:

- National Institute of Standards and Technology (NIST)
- Government Accountability Office (GAO)
- ISACA (previously known as the Information Systems Audit and Control Association)
- U.S. Department of Education, Privacy Technical Assistance Center (PTAC)[5]

Controls established

School districts have an important responsibility for maintaining the privacy of student data and for implementing and maintaining information security controls. Districts often rely extensively on computerized systems to support educational and mission-related operations and on information security controls to protect the sensitive data residing on those systems. While we found areas where improvements are needed, as discussed in the Audit Issues section, we also found the districts have generally established:

- A technology usage policy to facilitate access to district technology and to create a safe environment for using the technology, including promoting online safety, security, and confidentiality.
- Policies and procedures, including applicable parent/student forms, required to be in compliance with the FERPA data disclosure and usage provisions.
- The controls and processes required to be in compliance with the Children's Internet Protection Act (CIPA).
- Certain controls designed to help ensure the privacy of data and to help ensure the confidentiality, integrity, and availability of significant systems and data maintained on those systems.

[4] 5 CSR Section 20-700.100

[5] According to its web site, the U.S. Department of Education established the PTAC as a "one-stop" resource for education stakeholders to learn about data privacy, confidentiality, and security practices related to student-level longitudinal data systems. The PTAC provides information and guidance on privacy, confidentiality, and security practices through a variety of resources. PTAC information is available at <http://nces.ed.gov/programs/ptac>.

Certain districts have established additional controls. Refer to the individual audit reports, listed in the Appendix, for a list of controls established by each district.

Summary of Audit Findings
Cyber Aware School Audits
Audit Issues

1. Data Governance

A comprehensive data governance program has not been established or the program has not been completed. As a result, 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.

Continued growth in the amount of student data and information collected and stored electronically by school districts has increased the need for protecting and managing this data. Data governance is a set of processes that helps ensure sensitive data is formally managed so that student data is available to those that need it while at the same time ensuring individual student privacy is maintained. Data governance puts people in charge of ensuring that student data is accurate and protected from misuse.

According to the U.S. Department of Education, Privacy Technical Assistance Center (PTAC), data governance is necessary to ensure the confidentiality, integrity, availability, and quality of data. Establishing a data governance program is a critical task for any educational organization. An effective program requires establishing decision-making authority, defining policies and practices for the protection of sensitive data, identifying and gaining support of stakeholders, implementing the program, and monitoring its success. By clearly establishing policies, standard procedures, responsibilities, and controls for data activities, a data governance program helps to ensure that information is collected, maintained, used, and disseminated in a manner that protects privacy, confidentiality, and security, while allowing educational organizations to meet their missions.

Important components that districts have not incorporated into comprehensive data governance programs include:

- Responsibility for data management
- Data stewardship
- Inventory and classification of data
- Source and content of data
- Monitoring unauthorized disclosure of PII
- Archival and/or destruction of data at the end of its lifecycle

Without a formal data governance program, the district cannot ensure that sensitive and personally identifiable data maintained by the district is adequately protected and safe from unauthorized access, misuse, or inadvertent disclosure.

Recommendation

Establish and implement a formal data governance program encompassing the full life cycle of data, from acquisition to use to disposal.

2. User Accounts

Controls for creating and maintaining user accounts for accessing system resources have not been fully established.

Computer systems and data must be protected to prevent unauthorized access and misuse of sensitive data. A common way to manage access, and track who is using a system, is with user accounts to identify (user ID) and authenticate (password) users. User accounts can be used to control how much or to what parts of a system a user has access and the actions they can take while on a system. A district should have policies and procedures for authorizing, reviewing, and removing user access to systems and data and document such authorizations and actions. User account access controls should limit access to only the individuals who need such access to perform their job, remove accounts no longer necessary, and include a review of user access rights periodically.

2.1 Terminated users

Policies and procedures for disabling or removing user accounts timely after a user terminates have not been documented, or require additional steps. We found former users still had access to district systems and information 30 or more days after leaving the district.

Without effective procedures to remove access upon termination, former employees could continue to have access to critical or sensitive data and resources, increasing the risk of the unauthorized use, modification, or destruction of data and information.

Recommendation

Fully establish, document, and follow policies and procedures to ensure user accounts and related access privileges are removed timely upon user termination.

2.2 Account request

Policies and procedures for requesting, establishing, and maintaining user access to data and other system resources have not been formally documented. Additionally, a standard user access request form is not used to document the request and approval process.

To adequately control accounts, an organization should establish policies and procedures for authorizing and maintaining all user accounts, including system administrators. These policies and procedures should cover user access needed for routine operations, emergency access, and the sharing and disposition of data with individuals or groups outside the organization.

Without appropriate account access policies and procedures, users may be granted inappropriate or unauthorized access, which can provide opportunities for misuse or inappropriate disclosure of sensitive data.

Recommendation

Establish and document formal policies and procedures, including requiring standard forms, for requesting, approving, and maintaining access to systems.

2.3 Inactive account monitoring

Proactive monitoring for user accounts that have not been accessed or used for a specified period of time is not performed.

Inactive accounts can indicate users no longer need the access privileges provided by the accounts. Without appropriate monitoring, security administrators are less likely to identify user accounts that had not been accessed or used for a specified period of time.

Recommendation

Periodically monitor user account access to identify and evaluate inactive accounts.

2.4 Review of user access

Periodic reviews of users' access to data to ensure access remains appropriate and aligned with job duties have not been performed.

As users' work assignments and job responsibilities change, access rights to district systems may be added, changed, or removed. Over time, users can accumulate access rights that are no longer necessary, increasing the risk of inappropriate access to district data.

Without periodically reviewing user access rights, there is an increased risk that unauthorized alterations of the rights will go undetected or that access rights may not be aligned with current job duties.

Recommendation

Periodically review user access to data and other information resources to ensure access rights remain appropriate and are commensurate with job duties and responsibilities.

2.5 Shared accounts

Certain staff share user accounts and passwords. Because the accounts are shared, any actions taken by the account users cannot be identified with a specific user. Additional compensating controls, such as monitoring or management review of actions performed using these accounts, are not in place.

Allowing multiple users to share the same account, without establishing compensating controls, makes it difficult, if not impossible, to identify the user responsible for changes made to system settings.

Recommendation

Eliminate the use of shared accounts, or establish compensating monitoring controls to mitigate the risk of lack of individual accountability for system activity.

3. Security Controls

Not all necessary security controls have been implemented, leaving district technology assets, including personally identifiable information (PII), at risk of inappropriate access, use, and disclosure.

Security controls involve the management of people, processes, and technology to help protect a district's computer systems and data, including sensitive student data. Security controls are safeguards or countermeasures, such as strong passwords, to avoid, detect, counteract, or minimize security risks to computer systems, data, physical property, or other assets. Security controls involve establishing policies, supervision, manual processes, actions by individuals, or automated processes. Security controls can be built in to computer systems or devices to help protect data stored electronically or can help protect physical computer resources, such as laptops and network devices, by securing the areas where the resources are located.

3.1 Security administrator

Specific personnel have not been formally appointed to serve as security administrator or formally assigned responsibility for creating, implementing, and maintaining security policies and procedures.

The technology director and technology staff are often informally tasked with maintaining the security of technology resources and data. However, without a formal designation of staff responsible for security administration, there is increased risk that security policies and procedures may not be adequately designed, documented, implemented, and updated.

Recommendation

Formally appoint a security administrator who is responsible for developing and maintaining district security policies and procedures.

3.2 Password controls

Network passwords are not required to be periodically changed and controls to enforce the use of strong passwords are not required. As a result, there is less assurance passwords effectively limit access to computer systems and data files to only authorized users and those individuals who need access to perform their job responsibilities. Passwords should be changed periodically and strong password controls should be implemented to reduce the risk of unauthorized access to and use of systems and data.

Without requiring passwords to be periodically changed or enforcing strong password controls, there is an increased risk of a password becoming known by someone other than the account owner, which may result in inappropriate access to and misuse of sensitive district information.

Recommendation

Ensure passwords are periodically changed and enhance password controls to prevent unauthorized access to computers and data.

3.3 Access controls

Policies and procedures regarding user access to systems and data have not been fully established. As a result, certain access controls needed to protect systems have not been implemented.

Logon banners	Logon banners are not displayed to users accessing district systems and data. Logon banners should display information to system users regarding applicable privacy and security notices and required compliance with applicable laws, regulations, and policies. Without a displayed logon banner, users may not be informed or aware of the authorized or appropriate use of the system and data.
Concurrent users	Controls have not been established to limit or detect concurrent access to district systems. Concurrent session controls prevent a single user from accessing an information system from more than a specified number of locations at any given time. These controls help prevent unauthorized users from accessing the system by masquerading as an authorized user. Without limiting or detecting access from multiple locations at the same time, management may not be able to ensure the confidentiality, integrity, and availability of data and the system.
Recommendation	Fully establish access control policies and procedures by implementing logon banners for district systems to indicate appropriate use and by establishing security controls to manage and monitor the number of concurrent sessions for a single user.
3.4 Security logs	Policies and procedures to identify the types of security events to be logged and monitored have not been formally documented or the documented policies need to be enhanced. As a result, there is less assurance that detected and logged security incidents are properly investigated and resolved. Often, system default logging settings are used. Because districts have not customized these settings regarding which events are logged, the security logs are voluminous and cannot effectively be monitored for unusual or suspicious activity. A district should establish relevant criteria and identify significant system events that should be logged. At a minimum, all such significant events, including access to and modification of sensitive or critical system resources, should be logged. Also, logging should include appropriate information to facilitate monitoring of such significant system events. Without an effective method to identify, log, and monitor significant security-relevant events, a district is at increased risk that unauthorized or inappropriate system activity may not be detected.
Recommendation	Establish and document criteria for identifying which security events should be written to audit logs and monitored and investigated as security incidents.
3.5 Physical security	Physical security controls have not been fully established to ensure protection of technology resources. For example, responsibility for physical

security of technology resources has not been formally assigned; a documented policy for physical access to technology resources, including who can be authorized access to restricted or sensitive areas, has not been established; and keys to access restricted areas are not adequately controlled nor spare keys properly monitored.

Without adequate physical security controls, a district is at risk the physical infrastructure of the computer network could be accidentally or maliciously damaged, destroyed, or lost; causing significant issues for the district.

Recommendation

Formally document responsibility for physical protection of technology resources and develop policies and procedures to effectively restrict physical access.

3.6 Documentation of security controls

Policies and procedures for certain security controls have not been documented, including:

- Requesting and receiving approval for system access.
- User identification and password requirements for users accessing district technology resources.
- Procedures for establishing user access to data and other resources.
- Policies regarding which security groups users may be assigned to, along with the access rights granted each group.
- Policies describing who may be granted privileged access to systems.
- Resetting lost or compromised passwords.
- Notifying security administrators of the need to disable accounts for users terminating employment.
- Policies describing how to disable accounts for users terminating employment.
- Periodically reviewing user access to data and other information resources.
- Periodic reviews of user groups, including membership and the access rights granted to the groups.
- The allowable use of removable media, such as flash drives.

According to accepted standards, documentation of all aspects of computer support and operations is important to ensure continuity and consistency. Formalizing operational practices and procedures with sufficient detail helps to eliminate security lapses and oversights, gives new personnel sufficiently detailed instructions, and provides a quality assurance function to help ensure that operations will be performed correctly and efficiently.

Without documented and approved policies and procedures, management may not have assurance that control activities are appropriate and properly applied.

Recommendation

Fully document and periodically review security policies and procedures.

4. Incident Response and Continuity Planning

Additional measures are necessary to protect data in the event of a breach or other disruptive incident.

Security incidents and breaches of electronically-stored data are a growing concern for all organizations. Establishing and implementing an incident response plan, data breach response policy, and continuity plan outlining district policies and procedures for addressing potential incidents is an essential step in protecting the privacy of student data. Establishing these plans for detecting and responding to incidents, complete with clearly defined roles and responsibilities, provides a better response capability and can help shorten the incident response and recovery time. Prompt response helps minimize the risk of any further data loss and helps limit negative consequences of an incident or breach, including potential harm to individuals impacted by the incident. Continuity planning helps ensure that resources, including data, which has been lost, manipulated, or compromised; whether as the result of a cyberattack or a natural disaster; can be recovered quickly to minimize the impact on a district's operations.

4.1 Incident response documentation

Policies and procedures for responding to security incidents have not been formally documented.

According to accepted standards, a security incident is an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat or violation of security policies, security procedures, or acceptable use policies. It is important that an organization have formal written procedures for reporting security violations or suspected violations to a central security management office so that multiple related incidents can be identified, other employees alerted to potential threats, and appropriate investigations can be performed.

Without prompt and appropriate responses to security incidents, violations could continue to occur and cause damage to an organization's resources indefinitely. Further, violators will not be deterred from continuing inappropriate access activity, which could result in disclosure of confidential information and financial losses.

Recommendation

Establish and document an incident response plan that includes centrally tracking all security incidents.

4.2 Data breach response policy

A comprehensive data breach response policy has not been established. Implementing a data breach response policy is an essential step in protecting the privacy of student data.

A data breach is a security incident in which sensitive or confidential data, such as PII, has potentially been accessed, stolen, or used by an

unauthorized individual. The U.S. Department of Education, PTAC recommends all educational organizations create a data breach response policy. The policy should establish goals for the response process and include the definition of a breach, staff roles and responsibilities, as well as reporting, remediation, and feedback mechanisms. The policy should be well publicized and made easily available to all personnel whose duties involve data privacy and security protection.

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.

Recommendation

Formally document and adopt a comprehensive data breach response policy to promote an appropriate response in the event of a breach of protected student data.

4.3 Continuity planning

A complete continuity plan has not been documented and formally tested. Individuals responsible for carrying out those duties have not received formal training.

Elements of a continuity plan districts have not documented include:

- Priorities and procedures for the restoration of critical systems and data.
- Identification of persons responsible for restoration of specific systems and data.
- Formal identification of the resources and data included in the district's backups.

According to accepted standards, a continuity plan or suite of related plans should be developed for restoring critical business functions and applications. The plans should include arrangements for alternative processing facilities in case the usual facilities are significantly damaged or cannot be accessed. Staff should be trained and aware of their responsibilities to prevent, mitigate, and respond to emergency situations. Additionally, testing continuity plans is essential for determining whether the plans will function as intended in an emergency situation.

Without a tested and functional continuity plan, management has limited assurance the organization's business functions and computer processing can be sustained during or promptly resumed after a disruptive incident.

Recommendation

Develop a comprehensive continuity plan and formally assign responsibilities for development, implementation, and maintenance of the plan to appropriate personnel. Once established, ensure the plan is tested on a periodic basis.

5. Security Awareness Program

A formal security and privacy awareness training program has not been established. 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.

Technology solutions are not always the answer for preventing a security incident or a data breach. Establishing a district-wide security awareness training program is an effective way to make sure employees are aware of cyber threats so they will not make costly errors that could result in a security incident or data breach. Encouraging awareness about data protection and security issues while developing properly trained staff requires that various areas be addressed through a comprehensive training program. Security awareness training initiatives can include classroom style sessions, security awareness websites, helpful hints provided via email, and bulletin board notices. These methods can help ensure employees have a solid understanding of district security policies, procedures, and best practices and what they can do to recognize and respond appropriately to potential security issues and cyber threats.

According to accepted standards, the purpose of computer security awareness, training, and education is to (1) enhance security by improving awareness of the need to protect system resources and developing skills and knowledge so computer users can perform their jobs more securely; and (2) build in-depth knowledge, as needed, to design, implement, or operate security programs for organizations and systems. With proper security and privacy awareness training and clear communication of data and device use policies, employees can become the first line of defense against cybersecurity incidents.

Without adequate training, users may not understand system security risks and their role in implementing related policies and controls to mitigate those risks.

Recommendation

Establish a formal security and privacy awareness training program.

6. Vendor Controls

Controls for monitoring vendors and contracts have not been fully established.

Districts can obtain the use of information system services, including use of computer software and data backup services, through contracts and licensing agreements with vendors. Vendors should meet the same security requirements that the organization itself is required to meet when processing, storing, or transmitting information or operating information systems on behalf of an organization. The responsibility for managing risks from the use of a vendor's information system services remains with district officials. This risk can be managed by establishing thorough written

contracts and monitoring processes to ensure technology vendors comply with district security requirements.

6.1 Vendor monitoring

A process for ensuring software acquired or outsourced from information technology vendors complies with data security principles has not been established.

Software products from a number of vendors are used to manage financial information, human resources data, student data, and other information. Depending on the arrangement, some products are installed on district-owned equipment and maintained by district personnel (with additional support from the vendor), while others are hosted and maintained directly by the vendor. Contracts often contain a clause stating the vendor will provide appropriate security functionality for a district. However, district staff had not asked vendors to provide documentation that their product's security functionality met generally accepted industry standards.

Without an effective process for monitoring and managing risk of software acquisition or outsourcing, districts have less assurance in a vendor's ability to deliver services effectively, securely, and reliably and to ensure that services meet current and future data privacy and security needs.

Recommendation

Develop procedures to formally monitor information technology vendors to ensure the district's data is properly protected and the vendor acts in accordance with contract terms and conditions.

6.2 Vendor contracts

A written contract has not been established with the vendor of a critical district system or the contract does not fully define expectations over securing and accessing district data.

The U.S. Department of Education, PTAC provides best practices for organizations entering into written agreements. These best practices include stating ownership of PII; agreeing on limitations on use of PII, including restrictions on marketing, advertising, data mining; and maintaining data in a secure manner by applying appropriate technical, physical, and administrative safeguards to properly protect PII. They also include setting terms for data destruction, identifying penalties for inappropriate disclosure, and defining terms for conflict resolution.

Without a written contract that fully defines data security expectations, districts cannot ensure the security and privacy of its data, and cannot rely on enforceable contractual provisions in the event of a vendor dispute or noncompliance.

Recommendation

Establish a written contract and/or improve the existing contract with the vendor defining services provided and expectations over securing and accessing district data.

Summary of Audit Findings
Cyber Aware School Audits
Appendix - Audit Reports

Report Number	Title	Publication Date
2016-015	Boonville R-1 School District - Student Data Governance	March 2016
2016-025	Waynesville R-VI School District - Student Data Governance	May 2016
2016-058	Cape Girardeau Public School District - Student Data Governance	August 2016
2016-084	Park Hill School District - Student Data Governance	September 2016
2016-089	Orchard Farm R-V School District - Student Data Governance	September 2016