



Office of Missouri State Auditor
Nicole Galloway, CPA

Summary of Local Government and Court
Audit Findings - Information Security
Controls



Nicole Galloway, CPA
Missouri State Auditor

CITIZENS SUMMARY

Findings in the summary report of common cybersecurity mistakes

Background	This report examines local government and court compliance with some of the most basic data security practices. The State Auditor's Office compiled results of 30 local government and court audits issued by the office between July 2015 and June 2016, that contained cybersecurity concerns. This summary highlights the following five most common cybersecurity issues.
Access (User Access Management)	Employees and officials have access to more parts of computer systems than they need to perform their jobs. In 11 audit reports, auditors identified issues related to managing access to computer systems. Most of these issues involved access rights and privileges, which should be limited based on user needs and job responsibilities. Access rights and privileges are used to determine what a user can do after being allowed into the system. As an example, unrestricted access to a property tax system might allow unauthorized changes to property tax records.
Passwords (User Authentication)	Employees and officials share computer system passwords, do not have to change their passwords regularly, or do not have passwords for some of their computer systems. In 20 audit reports, auditors identified password issues. The majority of these findings were due to the lack of a requirement for passwords to be changed or passwords being shared between users. Individual users should have their own unique passwords, which should be changed periodically to reduce the risk of unauthorized access to and use of systems and data. Without these controls, the likelihood that accounts could be compromised and used by unauthorized individuals to gain access to sensitive information is increased.
System Locks (Security Controls)	Local governments and courts did not always have controls in place to lock access to a computer when an employee leaves it unattended or when someone tries to access it by guessing an employee's password. In 12 reports, auditors identified inadequate security controls. In most cases, inactivity controls have not been implemented to lock a computer or system after a certain period of inactivity or after a specified number of unsuccessful logon attempts. To reduce the risk of unauthorized individuals accessing an unattended computer and having potentially unrestricted access to programs and data files, users should log off computers when unattended and an inactivity control should be implemented to lock a computer or terminate a user session after a certain period of inactivity. Logon attempt controls should also lock the capability to access a computer or system after a specified number of consecutive unsuccessful logon attempts and are necessary to prevent unauthorized individuals from continually attempting to logon to a computer or system by guessing passwords.
Data Backups (Backup and Recovery)	Data is not being backed up on a regular basis in a secure off-site location and when the data is backed up, there are not regular tests to make sure the data can be restored in the system. In six audit reports, data in various systems was not periodically backed up, tested, stored offsite or accounted for as part of a disaster recovery plan. In some cases, data was not regularly backed up. In others, data backups were conducted, but not stored at an off-site location to reduce the risk of loss in the event of a disaster or other disruptive incident. Preparation of backup data, preferably on a daily or at

least weekly basis, provides reasonable assurance data could be recovered if necessary. In other cases, the data backups were not tested, which limits the assurance that backup systems will work properly when needed.

User Restrictions and
Tracking
(Data Management)

Government computer systems do not always have protections in place to prevent improper changes to information and do not have a way to track how changes were made. Data management was cited in 11 audit reports, which includes integrity controls to guard against the improper modification or destruction of data, and in the case of school districts, tracking mechanisms for school attendance records and changes. Data management controls lessen the risk for manipulation of data and provide additional information so changes can be traced back to a specific person.

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 Local Government and Court Audit Findings

Information Security Controls

Table of Contents

State Auditor's Report	2
------------------------	---

Audit Issues	
1. User Access Management	3
2. User Authentication.....	4
3. Security Controls.....	6
4. Backup and Recovery.....	8
5. Data Management.....	9

Appendix	
Audit Reports	11



NICOLE GALLOWAY, CPA
Missouri State Auditor

Honorable Jeremiah W. (Jay) Nixon, Governor
and
Members of the General Assembly
Jefferson City, Missouri

This report was compiled using local government and court audit reports issued by my office between July 2015 and June 2016 (report numbers 2015-045 through 2015-135 and 2016-001 through 2016-042). This summary excludes the two audit reports issued during this period as part of the Cyber Aware School Audits Initiative (report numbers 2016-015 and 2016-025). Those reports will be included in a separate summary for that initiative. The objective of this report was to summarize recent information security control issues and recommendations.

The recommendations address a variety of topics including user access management, user authentication, security controls, backup and recovery, and data management. The Appendix lists the 30 reports with findings covering these topics.

A handwritten signature in black ink that reads "Nicole R. Galloway".

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 Local Government and Court Audit Findings

Information Security Controls

Audit Issues

1. User Access Management

1.1 Access rights and privileges

Access to certain systems is not adequately restricted. Access rights and privileges are used to determine what a user can do after being allowed into a system, such as read or write to a certain file. Unrestricted system access allows the capability to make unauthorized changes to records or to delete or void transactions after the transactions have been entered in the system. In addition, adequate supervisory reviews of users are not performed. Access should be limited based on user needs and job responsibilities.

Without adequate user access restrictions, there is an increased risk of unauthorized changes to data and records and of the loss, theft, or misuse of funds.

Recommendation

Ensure user access rights are limited to only what is necessary to perform job duties and responsibilities.

Report Source

2015-054 (13th Judicial Circuit/Boone County)
2015-099 (Ralls County)
2015-116 (Village of Leasburg)
2015-117 (Phelps County)
2015-123 (Butler County)
2015-135 (29th Judicial Circuit/City of Joplin Municipal Division)
2016-018 (Madison County)
2016-033 (21st Judicial Circuit/City of Bella Villa Municipal Division)
2016-036 (Linn County)

1.2 Acceptable use agreements

Signed technology acceptable use agreement forms are not always maintained and the most current form was not always used. Students are required to sign this agreement when registering for school each year and copies are to be maintained at each school. Acceptable use agreements are used to acknowledge the procedures governing the acceptable use of computers, internet access, email and procedures designed to protect resources and confidential information.

Without using and maintaining the approved agreement forms, there is an increased risk students have not been provided with, reviewed, and agreed to comply with the most current policies necessary to reduce the risk of cybersecurity incidents.

Recommendation

Ensure current acceptable use agreement forms are used and maintained.

Report Source

2016-031 (Fox C-6 School District)



Summary of Local Government and Court Audit Findings
Information Security Controls
Audit Issues

1.3 Periodic review of user accounts

Periodic reviews of users' access to data and other information to ensure access remains appropriate and aligned with job duties are not performed. As users' work assignments and job responsibilities change, access rights to data 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 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

Ensure periodic reviews of user access to data and other information resources are performed to ensure access rights remain appropriate and are commensurate with job duties and responsibilities.

Report Source

2015-054 (13th Judicial Circuit/Boone County)
2015-135 (29th Judicial Circuit/City of Joplin Municipal Division)

1.4 Terminated employees

The user access of former employees is not disabled timely.

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

Recommendation

Ensure user access is promptly deleted following termination of employment to prevent unauthorized access to computer systems and data.

Report Source

2015-135 (29th Judicial Circuit/City of Joplin Municipal Division)
2016-027 (Stone County)

2. User Authentication

2.1 Passwords not changed

Passwords are not required to be changed on a periodic basis. As a result, there is less assurance passwords are effectively limiting access to computer systems and data files to only those individuals who need access to perform their job responsibilities. Passwords should be changed periodically to reduce the risk of unauthorized access to and use of systems and data.

Without requiring passwords to be periodically changed, the likelihood that accounts could be compromised and used by unauthorized individuals to gain access to sensitive information is increased.



Summary of Local Government and Court Audit Findings
Information Security Controls
Audit Issues

Recommendation

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

Report Source

2015-054 (13th Judicial Circuit/Boone County)
2015-068 (DeKalb County)
2015-079 (Grundy County)
2015-096 (Holt County)
2015-099 (Ralls County)
2015-100 (Warren County)
2015-114 (Hannibal School District #60)
2015-115 (Harrison County)
2015-116 (Village of Leasburg)
2015-123 (Butler County)
2015-126 (29th Judicial Circuit/City of Carl Junction Municipal Division)
2015-128 (City of Gallatin)
2015-133 (Henry County)
2016-010 (24th Judicial Circuit/City of Leadington Municipal Division)
2016-012 (Douglas County)
2016-021 (Marion County)
2016-024 (Ozark County)
2016-027 (Stone County)
2016-035 (Oregon County)

2.2 Sharing passwords

User accounts and passwords for accessing computers and various systems are shared by users. The security of a password system is dependent upon keeping passwords confidential. By allowing users to share accounts and passwords, individual accountability for system activity could be lost and unauthorized system activity could occur.

Without strong user account and password controls, including maintaining the confidentiality of passwords, the likelihood that accounts could be compromised and used by unauthorized individuals to gain access to sensitive information is increased.

Recommendation

Ensure unique user accounts and passwords are required to access computers and data. In addition, ensure users understand the importance of maintaining the confidentiality of passwords.

Report Source

2015-068 (DeKalb County)
2015-079 (Grundy County)
2015-099 (Ralls County)
2015-100 (Warren County)
2015-115 (Harrison County)
2015-116 (Village of Leasburg)
2015-123 (Butler County)
2015-126 (29th Judicial Circuit/City of Carl Junction Municipal Division)



Summary of Local Government and Court Audit Findings
Information Security Controls
Audit Issues

2016-021 (Marion County)
2016-024 (Ozark County)
2016-027 (Stone County)
2016-035 (Oregon County)
2016-036 (Linn County)

2.3 Password not required

A password is not required to logon and authenticate access to a computer.

Without requiring passwords to access a computer or system, there is no assurance the data or system is protected from unauthorized access and use.

Recommendation

Ensure passwords are required to authenticate access to computer systems and data.

Report Source

2016-027 (Stone County)

2.4 Password complexity

Passwords are not required to contain a minimum number of characters. Strong passwords are often the first line of defense into a computer or system. As a result, an appropriate minimum character length should be established so passwords cannot be easily guessed or identified using password-cracking mechanisms.

Without enforcing password complexity by requiring a minimum number of characters, there is an increased risk that passwords can be more easily guessed, allowing unauthorized access to data and systems.

Recommendation

Ensure passwords contain a minimum number of characters so they cannot be easily guessed.

Report Source

2016-024 (Ozark County)

3. Security Controls

3.1 Inactivity control

Inactivity controls have not been implemented to lock a computer or system after a certain period of inactivity. To reduce the risk of unauthorized individuals accessing an unattended computer and having potentially unrestricted access to programs and data files, users should log off computers when unattended and an inactivity control should be implemented to lock a computer or terminate a user session after a certain period of inactivity.

Without an inactivity control, there is an increased risk of unauthorized access to computers and the unauthorized use, modification, or destruction of data.



Summary of Local Government and Court Audit Findings
Information Security Controls
Audit Issues

Recommendation

Ensure an inactivity control is implemented to lock a computer or system after a certain period of inactivity.

Report Source

2015-068 (DeKalb County)
2015-114 (Hannibal School District #60)
2015-115 (Harrison County)
2015-133 (Henry County)
2016-012 (Douglas County)
2016-021 (Marion County)
2016-024 (Ozark County)
2016-027 (Stone County)

3.2 Unsuccessful logon attempts

Security controls have not been implemented to lock access to a computer or system after a specified number of unsuccessful logon attempts. Logon attempt controls lock the capability to access a computer or system after a specified number of consecutive unsuccessful logon attempts and are necessary to prevent unauthorized individuals from continually attempting to logon to a computer or system by guessing passwords.

Without effective controls to limit the number of consecutive unsuccessful logon attempts, there is less assurance sensitive data is effectively protected from unauthorized access.

Recommendation

Ensure a security control is implemented to lock access to a computer or system after multiple unsuccessful logon attempts.

Report Source

2015-068 (DeKalb County)
2015-099 (Ralls County)
2015-114 (Hannibal School District #60)
2015-128 (City of Gallatin)
2015-133 (Henry County)
2016-012 (Douglas County)
2016-021 (Marion County)
2016-024 (Ozark County)
2016-027 (Stone County)

3.3 Malware protection

Policies and procedures to ensure computer systems are adequately protected from malware (malicious code) have not been established and malware protection software to detect and eradicate malicious code has not been installed timely.

Without adequate malware protection, there is an increased risk that computers will be infected by malware and that unauthorized processes will have an adverse impact on the confidentiality, integrity, or availability of a system.



Summary of Local Government and Court Audit Findings
Information Security Controls
Audit Issues

Recommendation Ensure computers and systems are adequately protected from malware.

Report Source 2015-116 (Village of Leasburg)
2015-130 (Goodman Area Fire Protection District)

4. Backup and Recovery

4.1 Data backup Data in various systems is not periodically backed up. Preparation of backup data, preferably on a daily or at least weekly basis, provides reasonable assurance data could be recovered if necessary.

Without regular data backups, there is an increased risk critical data will not be available for recovery should a disruptive incident occur.

Recommendation Ensure data is regularly backed up.

Report Source 2015-130 (Goodman Area Fire Protection District)
2016-021 (Marion County)
2016-024 (Ozark County)

4.2 Off-site storage Data backups are not stored at a secure off-site location. Data backups are performed, however, the backups are stored at the same location as the original data leaving the backup data susceptible to the same damage as the original data.

Without storing backup data at a secure off-site location, critical data may not be available for restoring systems following a disaster or other disruptive incident.

Recommendation Ensure backup data is stored in a secure off-site location.

Report Source 2015-079 (Grundy County)
2015-099 (Ralls County)
2016-021 (Marion County)
2016-024 (Ozark County)
2016-027 (Stone County)

4.3 Periodic testing Periodic testing of backup data is not performed. Periodic testing of backups is necessary to ensure the backup process is functioning properly and to ensure all essential data can be recovered.

Without testing the full backup process, management cannot be assured the entire system can be restored when necessary.



Summary of Local Government and Court Audit Findings
Information Security Controls
Audit Issues

Recommendation Ensure backup data is tested on a regular, predefined basis.

Report Source 2015-079 (Grundy County)
2015-099 (Ralls County)
2016-024 (Ozark County)
2016-027 (Stone County)

5. Data Management

5.1 Data integrity Data integrity controls to guard against the improper modification or destruction of data and information have not been implemented. In addition, audit trail controls to provide evidence demonstrating how a specific transaction was initiated, processed, and recorded have not been established. As a result, critical systems, including accounting systems, property tax systems, and case management systems do not prevent users from manually entering dates or from changing check numbers and check dates in the systems once checks have been printed and issued. Also, critical systems do not prevent users from postdating or backdating receipts and checks or voiding and reissuing the same instrument number without a transaction audit trail being recorded. In addition, systems do not have the functionality to generate audit trail reports of receipts closed before being finalized or receipts voided by users after the transactions have been processed.

Without data integrity and audit trail controls, there is an increased risk of manipulation of data without detection and the loss, theft, or misuse of funds.

Recommendation Ensure adequate data integrity and audit trail controls are in place to allow for the proper accountability of all transactions.

Report Source 2015-048 (City of Kimberling)
2015-060 (City of Joplin)
2015-079 (Grundy County)
2015-115 (Harrison County)
2015-116 (Village of Leasburg)
2016-002 (45th Judicial Circuit/City of Winfield Municipal Division)
2016-021 (Marion County)
2016-027 (Stone County)
2016-036 (Linn County)

5.2 Student attendance data The attendance system does not limit the time frame during which changes can be made and there is no review by officials to ensure changes made to current school year attendance records are appropriate. In addition, an audit trail report of changes made is not generated and reviewed to ensure all changes made to attendance records are accurate and appropriate.



Summary of Local Government and Court Audit Findings
Information Security Controls
Audit Issues

Without limiting the time frame during which changes can be made or reviewing changes made, data is subject to erroneous changes that may significantly affect the reliability of official attendance reports.

Recommendation

Ensure student attendance data is accurately recorded and reported, including restricting the time frame during which changes can be made and ensure an audit trail of changes made to attendance data be prepared and reviewed for accuracy.

Report Source

2016-031 (Fox C-6 School District)

5.3 Numerical sequence

The numerical sequence of receipt numbers cannot be accounted for since the computerized system issues a sequential number for any action recorded in the system, including receipts, disbursements, and deposits.

Without adequate controls to account for the numerical sequence of receipt numbers, there is an increased risk of loss, theft, or misuse of funds.

Recommendation

Work with the computer software vendor to ensure adequate controls are in place to allow for proper accountability of all receipt numbers.

Report Source

2016-020 (Dunklin County)

5.4 Vendor contract

A written contract with a vendor providing information technology services has not been established. Clear and detailed written contracts, including reporting requirements and provisions to allow for proper monitoring, are necessary to ensure all parties are aware of their duties and responsibilities, prevent misunderstandings, and ensure monies are used appropriately and effectively. Additional terms should be included in contracts with information technology vendors to protect sensitive and confidential data.

Without a written contract, an organization 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

Ensure written contracts are established with vendors providing information technology services. Contracts should contain sufficient terms to limit access to and protect sensitive and confidential data.

Report Source

2015-048 (City of Kimberling)

Summary of Local Government and Court Audit Findings

Information Security Controls

Appendix - Audit Reports

Report Number	Title	Publication Date
2015-048	City of Kimberling	July 2015
2015-054	13th Judicial Circuit/Boone County	July 2015
2015-060	City of Joplin	August 2015
2015-068	DeKalb County	September 2015
2015-079	Grundy County	September 2015
2015-096	Holt County	October 2015
2015-099	Ralls County	November 2015
2015-100	Warren County	November 2015
2015-114	Hannibal School District #60	November 2015
2015-115	Harrison County	November 2015
2015-116	Village of Leasburg	November 2015
2015-117	Phelps County	November 2015
2015-123	Butler County	December 2015
2015-126	29th Judicial Circuit/City of Carl Junction Municipal Division	December 2015
2015-128	City of Gallatin	December 2015
2015-130	Goodman Area Fire Protection District	December 2015
2015-133	Henry County	December 2015
2015-135	29th Judicial Circuit/City of Joplin Municipal Division	December 2015
2016-002	45th Judicial Circuit/City of Winfield Municipal Division	January 2016
2016-010	24th Judicial Circuit/City of Leadington Municipal Division	March 2016
2016-012	Douglas County	March 2016
2016-018	Madison County	April 2016
2016-020	Dunklin County	April 2016
2016-021	Marion County	April 2016
2016-024	Ozark County	May 2016
2016-027	Stone County	May 2016
2016-031	Fox C-6 School District	May 2016
2016-033	21st Judicial Circuit/City of Bella Villa Municipal Division	June 2016
2016-035	Oregon County	June 2016
2016-036	Linn County	June 2016
