Nicole R. Galloway, CPA

Missouri State Auditor

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

October 2015

Report No. 2015-097

http://auditor.mo.gov

Nicole R. Galloway, CPA
Missouri State Auditor

CITIZENS SUMMARY

Summary 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 examined audits released in fiscal year 2015 and this summary highlights the following five most common cybersecurity issues.

1. Passwords

Government 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, password issues were identified. 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.

2. Access

Employees and officials have access to more parts of government computer systems than they need to perform their jobs. In 15 audit reports, there were issues related to managing access to computer systems. Most of these issues related to 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.

3. System Locks

Government computer systems do not always have programs in place to lock access to the computer when an employee leaves the computer unattended or when someone tries to guess the employee's password. In seven 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.
4. Data Backups	**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 seven 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 offsite 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.
5. User Restrictions and Tracking	**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 four 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.

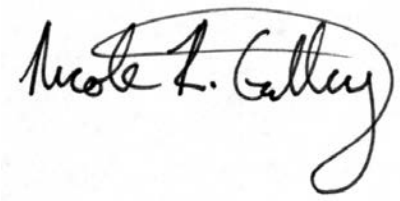
Summary of Local Government and Court Audit Findings
Information Security Controls
Table of Contents

NICOLE R. 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 between July 2014 and June 2015 (report numbers 2014-047 through 2014-143 and 2015-001 through 2015-044). 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 33 reports with findings covering these topics.



Nicole R. Galloway, CPA
State Auditor

The following auditors participated in the preparation of this report:

Deputy State Auditor:	John Luetkemeyer, CPA
Director of Audits:	Douglas J. Porting, CPA, CFE
	Regina Pruitt, CPA
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 the 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

2014-051 (First Judicial Circuit/Clark County)
2014-058 (Atchison County)
2014-060 (Fourth Judicial Circuit/Atchison County)
2014-061 (Twenty-Sixth Judicial Circuit/Laclede County)
2014-095 (Webster County)
2014-104 (Lewis County Collector and Property Tax System)
2014-109 (Miller County)
2014-113 (Howell County)
2014-120 (Iron County)
2014-123 (Seventeenth Judicial Circuit/Cass County)
2014-136 (Shannon County)
2015-025 (Butler County Collector and Property Tax System)
2015-044 (Second Judicial Circuit/Adair County)

1.2 Access request forms

Access request forms or other written documentation is not used for requesting and approving access to information assets. To control access, a standardized form should be used showing documented authorizations of access rights for all users.

Without documented approvals of user access rights, there is an increased risk of unauthorized access.

Recommendation

Ensure a standard form for requesting and authorizing access to information assets is used.

Report Source

2015-002 (Jefferson College)

1.3 Terminated employees

The user access of former employees was 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

2014-051 (First Judicial Circuit/Clark County)
2014-094 (Texas 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.

Recommendation

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

Report Source

2014-052 (Livingston County Collector-Treasurer and Property Tax System)
2014-062 (Grandview C-4 School District)
2014-080 (Andrew County)
2014-094 (Texas County)
2014-113 (Howell County)
2014-119 (Clinton County)
2014-125 (Osage County)
2014-127 (Scott County)
2014-135 (Perry County)
2014-139 (City of Kimmswick)
2015-002 (Jefferson College)
2015-006 (St. Joseph School District)
2015-007 (City of Dixon)
2015-009 (Clinton County Collector and Property Tax System)
2015-017 (Twenty-Fifth Judicial Circuit/City of Dixon Municipal Division)
2015-021 (Hickory County)

2015-024 (Barry County)
2015-043 (Adair 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

2014-051 (First Judicial Circuit/Clark County)
2014-094 (Texas County)
2014-113 (Howell County)
2014-119 (Clinton County)
2014-125 (Osage County)
2014-127 (Scott County)
2014-139 (City of Kimmswick)
2015-007 (City of Dixon)
2015-009 (Clinton County Collector and Property Tax System)
2015-024 (Barry County)
2015-037 (Schuyler 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

2014-135 (Perry 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.

Recommendation

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

Report Source

2014-051 (First Judicial Circuit/Clark County)
2014-052 (Livingston County Collector-Treasurer and Property Tax System)
2014-062 (Grandview C-4 School District)
2014-125 (Osage County)
2014-135 (Perry County)
2015-007 (City of Dixon)

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

2014-052 (Livingston County Collector-Treasurer and Property Tax System)
2014-062 (Grandview C-4 School District)
2014-080 (Andrew County)
2014-125 (Osage County)
2015-007 (City of Dixon)

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

2014-109 (Miller County)
2015-017 (Twenty-Fifth Judicial Circuit/City of Dixon Municipal Division)
2015-037 (Schuyler County)

4.2 Offsite 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

2014-062 (Grandview C-4 School District)
2014-125 (Osage County)
2014-139 (City of Kimmswick)
2015-037 (Schuyler 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 backups, management cannot be assured the entire system can be restored when necessary.

Recommendation

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

Report Source

2014-125 (Osage County)
2014-139 (City of Kimmswick)
2015-006 (St. Joseph School District)

4.4 Disaster recovery plan

Management has not developed a disaster recovery plan to ensure computer operations can be promptly restored in the event of a disaster or other disruptive incident. A comprehensive written disaster recovery plan should include plans for a variety of disaster situations and specify detailed recovery actions required to reestablish critical computer and network operations. Once a disaster recovery plan has been developed and approved, the plan should be periodically tested and reviewed.

Without an up-to-date and tested disaster recovery plan, management has limited assurance the organization's computer operations can be promptly restored after a disruptive incident.

Recommendation

Develop a comprehensive disaster recovery plan and periodically test and evaluate the plan.

Report Source

2015-006 (St. Joseph School District)

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 and property tax systems, do not prevent users from changing check numbers and check dates in the systems once checks have been printed and issued and do not prevent users from postdating or backdating receipts and checks without a transaction audit trail being recorded.

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

2014-047 (Taney County)
2014-104 (Lewis County Collector and Property Tax System)

5.2 Student attendance data

The attendance system does not adequately track some changes made to attendance records, 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.

Without limiting the time frame during which changes can be made or reviewing changes made, the data is subject to erroneous changes that may significantly affect 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

2015-012 (Joplin Schools)

5.3 Numerical sequence

The numerical sequence of transaction numbers assigned by the computerized accounting system is not accounted for.

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

Recommendation

Ensure adequate controls are in place to allow for proper accountability of all transactions numbers.

Report Source

2014-095 (Webster County)

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

Report Number	Title	Publication Date
2014-047	Taney County	July 2014
2014-051	First Judicial Circuit/Clark County	July 2014
2014-052	Livingston County Collector-Treasurer and Property Tax System	July 2014
2014-058	Atchison County	August 2014
2014-060	Fourth Judicial Circuit/Atchison County	August 2014
2014-061	Twenty-Sixth Judicial Circuit/Laclede County	August 2014
2014-062	Grandview C-4 School District	August 2014
2014-080	Andrew County	September 2014
2014-094	Texas County	October 2014
2014-095	Webster County	October 2014
2014-104	Lewis County Collector and Property Tax System	November 2014
2014-109	Miller County	November 2014
2014-113	Howell County	November 2014
2014-119	Clinton County	November 2014
2014-120	Iron County	December 2014
2014-123	Seventeenth Judicial Circuit/Cass County	December 2014
2014-125	Osage County	December 2014
2014-127	Scott County	December 2014
2014-135	Perry County	December 2014
2014-136	Shannon County	December 2014
2014-139	City of Kimmswick	December 2014
2015-002	Jefferson College	January 2015
2015-006	St. Joseph School District	February 2015
2015-007	City of Dixon	February 2015
2015-009	Clinton County Collector and Property Tax System	February 2015
2015-012	Joplin Schools	February 2015
2015-017	Twenty-Fifth Judicial Circuit/City of Dixon Municipal Division	April 2015
2015-021	Hickory County	April 2015
2015-024	Barry County	April 2015
2015-025	Butler County Collector and Property Tax System	April 2015
2015-037	Schuyler County	June 2015
2015-043	Adair County	June 2015
2015-044	Second Judicial Circuit/Adair County	June 2015