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