Susan Montee, CPA

Missouri State Auditor

TRANSPORTATION

Information Systems Security Controls

August 2008

Report No. 2008-49

auditor.mo.gov

Susan Montee, CPA
Missouri State Auditor

YELLOW SHEET

Missing Security Controls Leaves Technology Resources Susceptible to Threats and Vulnerabilities

This audit reviewed the management and control of information technology resources at the Missouri Department of Transportation (MoDOT). Auditors found MoDOT management has not taken some necessary steps to fully maintain effective controls to protect the confidentiality, integrity and availability of data and the information technology resources supporting the mission and operations of the department.

Risk assessment program is not implemented	MoDOT management has not established or documented risk management and assessment policies and procedures. A risk assessment helps identify potential threats and vulnerabilities or weaknesses that could be exploited and to ensure appropriate controls are implemented to mitigate these vulnerabilities. (See page 5)
Disaster recovery plan needed	MoDOT personnel have documented, approved and implemented a business continuity plan. However, Information Systems Division personnel have not established a disaster recovery plan to ensure the availability of technology resources. Without an operational disaster recovery plan, management does not have assurance that computer operations could be promptly restored in the event of a significant disruption to normal system operations. (See page 5)
Security management program is not fully implemented	A security management program provides a framework for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of an agency's security controls. MoDOT management has developed and documented policies and procedures for some security controls. However, management has not completed the process of establishing and documenting policies and procedures for other key security controls. Accepted standards state policies are necessary to set organizational strategic directions for security and assign resources for the implementation of security. (See page 6)

Contents

Abbreviations

GAO	Government Accountability Office
ISD	Information Systems Division
MoDOT	Missouri Department of Transportation
SAO	State Auditor's Office

SUSAN MONTEE, CPA
Missouri State Auditor

Honorable Matt Blunt, Governor
and
Missouri Highways and Transportation Commission
and
Pete K. Rahn, Director
Department of Transportation
Jefferson City, MO

The Missouri Department of Transportation (MoDOT) is responsible for maintaining the state's transportation systems, including the highway system. The Information Systems Division is responsible for providing technical assistance to support MoDOT technology resources. Our audit objective included determining whether MoDOT management established adequate policies and procedures to implement effective security controls to ensure the confidentiality, integrity, and availability of information maintained in MoDOT information systems.

MoDOT management has not taken some necessary steps to fully implement effective internal controls to prevent the unauthorized use and disclosure of data and to adequately protect information technology resources. Staff had not performed a formal risk assessment to identify potential threats and vulnerabilities to the department's data, systems and resources and the likelihood of occurrence. Management had implemented a business continuity plan but had not established a disaster recovery plan necessary to sustain and recover critical technology services following an emergency. Also, policies had not been developed for some key security controls, while for other controls, procedures had been established but the corresponding policies had not been documented.

We conducted our audit in accordance with the standards applicable to performance audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States. Those standards require that we plan and perform our audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides such a basis. This report was prepared under the direction of John Luetkemeyer. Key contributors to this report included Jeff Thelen, Lori Melton, and Richard Mosha.

Susan Montee, CPA
State Auditor

Introduction

The Missouri Department of Transportation (MoDOT) is responsible for developing, building, and maintaining the roads and bridges of the state highway system; administering other transportation programs, such as aviation, rail, public transit, waterways and bicycle/pedestrian; managing motor carrier operations; and providing other services. At February 2008, MoDOT had approximately 7,200 employees.[1] The MoDOT Information Systems Division (ISD) supports the department's mission through technological solutions and electronic communications. Information, some of which is sensitive, maintained in MoDOT systems includes:

- Commercial vehicle permits
- Personnel information, including social security numbers and benefit information
- Department expenditure records
- Fleet vehicle information
- Construction projects

According to accepted standards, security controls are the management, operational, and technical safeguards or countermeasures prescribed for an information system[2] to protect the confidentiality, integrity, and availability of the system and its information. Confidentiality refers to preserving authorized restrictions on information access and disclosure, including 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.

Scope and Methodology

To determine whether MoDOT management established internal control policies and procedures and implemented security controls, we conducted interviews with appropriate officials and staff; requested and reviewed available policies, procedures, and other applicable information; and performed testing.

We obtained data files from ISD of the various user accounts having access to MoDOT's networks as of April 2008. To ensure completeness of the data, we grouped the accounts by division/district code, compared the listing to the MoDOT organization chart, reviewed the accounts for reasonableness and scanned the names of the employees. We reviewed the last login date of

[1] A MoDOT official said 6,350 of these employees are salaried and the remainder work hourly as needed for the department (for example, in snow removal).

[2] Accepted standards define an information system as a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

the user accounts to identify inactive accounts. We provided an ISD official with a list of inactive accounts identified.

We obtained the employment records for MoDOT employees for fiscal years 2001 through 2008 from the statewide accounting system for human resources. We did not perform specific procedures to ensure reliability because the risk of unreliable results was considered immaterial. We matched this data to the user accounts to determine if any terminated employees had active user accounts. We provided an ISD official with a list of all user accounts we identified that were associated with terminated employees.

We also evaluated major department information systems to identify a single system for a subsequent audit.

We based our work on accepted state, federal, national and international standards and best practices related to information technology security controls from the following sources:

- Missouri Adaptive Enterprise Architecture[3]
- National Institute of Standards and Technology (NIST)
- U.S. Government Accountability Office (GAO)
- IT Governance Institute Control Objectives for Information and related Technology (COBIT)

[3] The Enterprise Architecture includes standards, policies and guidelines established by the Office of Administration, Information Technology Services Division. The Enterprise Architecture is made up of several information technology domains, including domains dedicated to security and information. The domains are not fully developed, but define the principles which are needed to help ensure the appropriate level of protection for the state's information and technology assets.

Missing Security Controls Leaves Technology Resources Susceptible to Threats and Vulnerabilities

MoDOT information technology resources are susceptible to threats and vulnerabilities including unauthorized use and disclosure of data and insufficient protection of technology assets. This situation has occurred because MoDOT management had not (1) performed a formal risk assessment to identify possible threats and the likelihood of occurrence, (2) developed and implemented a disaster recovery plan to ensure the availability of technology resources, and (3) fully implemented a security management program. In addition, key policies and procedures for internal controls, including security, had not been documented or had not been developed. Collectively, these weaknesses impair MoDOT's ability to ensure information technology resources are properly protected and the risk of threats and vulnerabilities are reduced to an acceptable level.

Risk Assessment Program Is Not Implemented

MoDOT management has not established or documented risk management and assessment policies and procedures. An ISD official said a business impact analysis is planned for fiscal year 2009. This analysis is one step of a risk assessment program, according to accepted standards. The official said department staff did not have the expertise to perform a full risk assessment.

Identifying and assessing information security risks are essential steps in determining what controls are required and what level of resources should be expended on controls. Moreover, by increasing awareness of risks, these assessments generate support for the adopted policies and controls, which helps ensure policies and controls operate as intended, according to GAO. A risk assessment helps identify potential threats and vulnerabilities or weaknesses that could be exploited and to ensure appropriate controls are implemented to mitigate these vulnerabilities.

Disaster Recovery Plan Needed

MoDOT personnel have documented, approved and implemented a business continuity plan. However, ISD personnel have not established a disaster recovery plan to ensure the availability of technology resources. An ISD official said disaster recovery planning is now a priority of the division and the department will receive $2 million for recovery efforts in fiscal year 2009. The official said completing the disaster recovery plan will be a multi-stage process with the first stage being completed by the end of June 2009. Without an operational disaster recovery plan, management does not have assurance that computer operations could be promptly restored in the event of a significant disruption to normal system operations.

Contingency planning is designed to mitigate the risk of system and service unavailability by focusing effective and efficient recovery solutions. Ultimately, an organization would use a suite of plans to properly prepare response, recovery, and continuity activities for disruptions affecting the

organization's information systems, business processes, and facilities, according to accepted standards.

Security Management Program Is Not Fully Implemented

A security management program provides a framework for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of an agency's security controls. A security management program is the foundation of an agency's security control structure and a reflection of management's commitment to addressing security risks. According to GAO, implementing a security program is essential to ensuring controls over information and information systems work effectively on a continuing basis.

MoDOT and ISD management have developed and documented policies for some security controls. However, officials have not completed the process of establishing and documenting policies and procedures for other key security controls. Accepted standards state policies are necessary to set organizational strategic directions for security and assign resources for the implementation of security.

MoDOT needs to develop policies for critical security controls

MoDOT management had not established or documented policies or procedures for the following critical security controls:

- User account review
- Security activity logging and monitoring
- Additional security settings
- Security awareness program
- Periodic background reinvestigation

Management needs to require reviews of user accounts

MoDOT and ISD management do not have a process in place to perform reviews of user access to data and other information resources to determine whether the access rights remain commensurate with job responsibilities. According to accepted standards, there should be regular reviews of all user accounts and related privileges. Requiring a review of all user accounts ensures the right type and level of access has been provided. Otherwise, user accounts and accesses can be granted to or maintained for users who should not have access, according to accepted standards. ISD officials said some divisions or application owners review access rights for their users, but this is not a universal policy. During our review of network user accounts, we identified:

- 263 network accounts for former employees
- 630 network accounts that had never been accessed
- 737 network accounts that had not been accessed in over 90 days, including 483 that had not been accessed in over a year

The state's enterprise architecture and accepted standards state agencies should have procedures to disable user access when a user leaves employment and to identify inactive or idle accounts. MoDOT and ISD policies require access to information technology resources be deactivated when an authorized user terminates employment. The policy does not address inactive accounts; however, an ISD staff person stated inactive user accounts are informally reviewed on a periodic basis. Unauthorized access to MoDOT's information resources through an account for a terminated employee or an inactive account may compromise the confidentiality and integrity of data maintained by the department.

Policy needed to review system security logs

ISD management has not taken sufficient steps to ensure system security controls have functioned properly. Policies and procedures for logging appropriate security-related events and monitoring specific access are necessary when developing effective security programs. Accepted standards state a logging and monitoring function enables the early detection of unusual or abnormal security activity[4] that may need to be addressed to ensure the approved security level is maintained.

MoDOT's network has system security logging capabilities to identify security events. An ISD official said the department has procedures in place to review external access to the department's network, but internal network security activity is not monitored. Policies and procedures for monitoring, reviewing and investigating the internal access logs have not been established. An ISD staff person said logs are only reviewed when a violation is brought to management's attention through other means. A survey performed in 2008[5] suggested development of ways to recognize potential threats based on the results of auditing, monitoring and tracking. This survey also emphasized the usefulness of regularly reviewing application, system and network logs for events that are outside of the norm.

Determining what, when, and by whom specific actions have been taken on a system is crucial to establishing individual accountability, investigating security violations, and monitoring compliance with security policies, according to GAO.

[4] Security activity includes users attempting to access data they are not authorized to access, performing a task they are not authorized to perform, or accessing data they are authorized to access that is of a sensitive nature.

[5] "Insider Threat Study: Illicit Cyber Activity in the Government Sector", *United States Secret Service, National Threat Assessment Center and CERT® Program, Software Engineering Institute at Carnegie Mellon University*, <http://www.cert.org/archive/pdf/insiderthreat_gov2008.pdf>, accessed May 22, 2008.

Additional security settings could limit vulnerability	MoDOT ISD policy allows a maximum time limit for locking inactive workstations that exceeds state guidance and does not limit the number of concurrent sessions for a single user. An ISD official said division staff increased the maximum time limit in the policy as a result of user complaints. The 60 minute limit exceeds state enterprise architecture guidance of a maximum of 30 minutes of inactivity. An ISD official said he was not aware concurrent sessions could be limited. According to accepted standards, the number of concurrent sessions for a user should be limited. Without these additional security settings, management may not be able to ensure the confidentiality, integrity, and availability of data and the system.
Employees do not receive ongoing security awareness training	Training is an essential component of a security program. Computer intrusions and security breakdowns often occur because computer users fail to take appropriate security measures. For this reason, it is vital employees using computer resources be aware of the importance and sensitivity of information they handle, as well as business and legal reasons for maintaining its confidentiality, integrity, and availability, according to GAO. An ISD official said personnel had not been trained on an ongoing basis regarding computer security and their roles in ensuring appropriate use of department resources. New employees receive informal security training as part of orientation, but employees do not receive any other security awareness training. According to accepted standards, employees play a crucial role in helping ensure the security of computer systems and information technology resources. Accepted standards also state ongoing training programs are necessary to maintain employees' security awareness to the level required to perform effectively.
Backgrounds of current employees not reviewed periodically	MoDOT does not perform periodic background reinvestigations on current employees who are working in sensitive positions. According to accepted standards, background checks should be performed for new employees and periodically for current employees, dependent on the sensitivity and/or criticality of the job function. A MoDOT official said MoDOT has established procedures to verify the background of all new employees and those that transfer to a new position in MODOT to identify any background concerns. In addition, contractors' backgrounds are reviewed when the contractor starts working with MoDOT and annually thereafter, according to an ISD official. However, both officials said there is no periodic reinvestigation of current employees.

Documented policies and procedures are needed for established security measures

MoDOT management established, but had not documented, policies and procedures for the following security controls:

- Data ownership
- Backup procedures
- Segregation of duties
- Containment strategies
- Review of policies

An ISD official said ISD has not documented these procedures because division efforts have been focused on delivery of projects and services. Undocumented policies increase the risk of the procedures being applied incorrectly and inconsistently.

Data and information owners' responsibilities need to be formally documented

MoDOT management has appointed information owners who make decisions about system access rights and application changes. However, policies have not been documented regarding the assignment and responsibilities of the owners. Accepted standards state the responsibilities and accountability of owners of computer systems should be explicit. Without having documented policies and procedures establishing data and information ownership responsibilities, there is an increased risk data and information assets will not be properly protected against unauthorized access.

Backup procedures are not documented

ISD management ensures MoDOT data, applications and systems are backed up on a regular basis. However, these backup procedures have not been documented. Accepted standards require management define, implement, and document procedures for backup and restoration of systems, applications, data and documentation in line with business requirements and the continuity plan.

Policies needed to ensure segregation of duties

Inadequately segregated duties increase the risk that erroneous or fraudulent transactions could be processed, improper program changes implemented, or computer resources damaged or destroyed, according to GAO. Although duties have been informally segregated, there is not a documented policy requiring an identification of incompatible duties or a policy requiring segregation of duties among information technology staff, according to an ISD official. Accepted standards state policies should be established to require a division of roles and responsibilities that should exclude the possibility for a single individual to subvert a critical process.

Strategies need to be documented for containing a security incident

Criteria and strategies for containing a security incident should be clearly documented to facilitate quick and effective decision-making, according to accepted standards. ISD officials said ISD has informally identified

containment strategies, but has not documented and formally approved these strategies. According to accepted standards, when a computer security incident has been detected and analyzed, it is important to contain it before the spread of the incident overwhelms resources or the damage increases. Without documented strategies, procedures for containing the incident may be difficult to determine.

MoDOT needs policies to review key standards and policies

The relevance of policies to support information technology strategy should be confirmed and approved regularly, according to accepted standards. According to ISD officials, an informal procedure is in place and a team has been established to review documented policies and revise as necessary. However, the officials said these procedures have not been documented. Without documented and approved policies and procedures to guide the review process, it is more difficult for management to be assured system, technological, or organizational environments are adequately addressed.

MoDOT needs to establish and document a configuration management process

ISD management has not implemented or documented a policy to ensure all configuration management[6] control measures are in place. ISD has documented a change management policy, but this policy does not fulfill guidelines for configuration management. According to accepted standards, an effective configuration management process includes configuration identification, configuration change control, configuration inventories, configuration monitoring, and patch management.[7] We found ISD management had not implemented or documented procedures for the following areas:

- Configuration identification
- Configuration monitoring
- Patch management

Configuration baselines not documented for all computer assets

Management should ensure a current baseline of computer system configurations is documented, according to accepted standards. ISD staff has not established a checklist of how to configure or a baseline configuration of the current settings for various computer assets.[8] Without

[6] Configuration management involves the identification and management of security features for all hardware and software components of an information system at a given point and systematically controls changes to that configuration during the system's life cycle, according to accepted standards.

[7] Patch management is the process of applying software patches to correct flaws. A patch is a piece of software code that is inserted into a program to temporarily fix a defect. Patches are developed and released by software vendors when vulnerabilities are discovered.

[8] We discussed the specific assets with ISD management.

an inventory of all computer assets and their configurations, management cannot adequately analyze and test controls.

Configuration settings need review

Current configuration information should be routinely monitored for accuracy and to ensure that the technology resource is functioning as intended, according to accepted standards. The division's change management policy requires approval for all changes before they are put in place. However, ISD staff said configuration settings are reviewed only by the individuals that have access to make setting changes and not an independent party. According to accepted standards, there should be a division of roles and responsibilities that reduces the possibility for a single individual to subvert a critical process. A configuration management system that enforces strict monitoring, follow-through and separation of duties can help identify implementation errors or unauthorized changes.

Patch management policies need to be documented

Accepted standards recommend all organizations have a systematic, accountable, and documented process for managing exposure to vulnerabilities through the timely deployment of patches. According to the state's enterprise architecture, patch management should include duties such as monitoring sources for vulnerabilities and threats; prioritizing and testing remediation; deploying patches; and verifying vulnerabilities have been successfully remediated. ISD staff manage patches, but management has not documented the policies and procedures. Without having a systematic, accountable, and documented patch management process for limiting exposure to vulnerabilities, there is an increased risk that software vulnerabilities can be exploited.

Conclusions

MoDOT management has not taken some necessary steps to fully implement effective internal controls to prevent the unauthorized use and disclosure of data and to adequately protect information technology resources. MoDOT management does not have assurance appropriate controls are in place to reduce risks of threats and vulnerabilities to an acceptable level since a formal risk assessment has not been performed. The recovery of services, systems and technology resources may be delayed following a disruption in operations or a disaster since MoDOT management had not established a disaster recovery plan. MoDOT's control environment is missing important security components because management has not fully implemented a security program. Important security controls have not been established or have been developed but lack documented policies and procedures to provide consistent guidance. Faced with the challenge of protecting systems and resources from continuing threats, vulnerabilities, and data breaches, MoDOT management should support establishing and documenting the controls necessary to ensure the

confidentiality, integrity, and availability of data and information collected and maintained by MoDOT.

Recommendations

We recommend the Director of the Department of Transportation:

2.1 Implement and document a risk management and assessment framework, which includes policies, standards, and procedures for performing periodic risk assessments so management can better protect the department's resources and its ability to perform the department's missions.

2.2 Document and approve a disaster recovery plan. The plan should then be tested and implemented to ensure computer operations could be promptly restored in the event of a disruption.

2.3 Close accounts assigned to former employees and review the need for the unused and inactive accounts.

2.4 Design, develop, and approve a security management program that provides a framework upon which department-wide security policies, standards, and procedures are formulated, implemented, and monitored. At a minimum, management should implement security controls and document policies and procedures by taking the following actions:

- Establish and document policies to periodically review user access to data and other information resources to ensure access rights are commensurate with user's job duties and responsibilities. The reviews of user accounts should also include procedures to determine if users are current or terminated employees and have an active or inactive account.
- Establish and document policies and procedures to periodically review security logs and potential violations.
- Establish security settings consistent with state guidance and accepted standards which would include locking workstations after a maximum period of inactivity of 30 minutes and limiting the number of concurrent sessions for a single user.
- Establish an ongoing security awareness training program to communicate department security policies to all employees on a periodic basis.
- Identify employees' positions considered sensitive and perform periodic background screenings.
- Document the responsibilities of data and information owners.
- Document the procedures to backup department data, applications and systems.

- Document policies and procedures to ensure adequate segregation of incompatible duties.
- Document the strategies and procedures for containing a security incident.
- Document a formal process to periodically review and re-approve key standards, directives, and policies and procedures.
- Establish and document a configuration management process. This process should include an inventory for all computer assets and their corresponding configuration settings, a requirement that configuration settings be routinely monitored by appropriate personnel, and a patch management process.

Agency Comments

2.1 MoDOT concurs with the recommendation to implement and document a risk management and assessment framework. MoDOT currently assesses risk daily by utilizing strong risk prevention tools and processes monitored by staff. MoDOT also responds to issues with stronger prevention techniques and incorporates vendor recommendations from specific assessments where appropriate. MoDOT has also previously participated in a formal risk assessment completed February 3, 2006, by Cyber Security and coordinated by the Office of Administration, Information Technology Services Division. This assessment was reviewed by the SAO. MoDOT will develop a policy and supporting standards and procedures that comprise a risk management and assessment framework by June 30, 2009.

2.2 MoDOT concurs with the recommendation to document and approve a disaster recovery plan. As of May 30, 2008, MoDOT relocated redundant data backup systems to an off-site location. Since fiscal year 2007, MoDOT has also been working on a multi-year Disaster Recovery program. Funding for fiscal year 2009 has been approved and efforts are underway. A written disaster recovery plan is to be completed by June 30, 2009 as part of the Disaster Recovery program.

2.3 MoDOT concurs with the recommendation to close inactive user accounts. As of July 11, 2008, MoDOT has disabled the former employee accounts and will have the remaining inactive accounts disabled no later than August 31, 2008. A process has been implemented to dynamically provide information regarding terminated employees for timely disabling of accounts. Additional procedures and processes are currently being implemented to assist in the monitoring and review of user accounts. This will be completed no later than December 31, 2008. MoDOT is also researching tools to assist in automating this effort.

2.4 MoDOT concurs with the recommendation to design, develop, and approve a security management program. MoDOT has assigned information security responsibilities to a staff designee and created in January 2008 an Information Systems Security Team. These roles have the responsibility of designing, and developing a security management program to be completed by June 30, 2010. We will consider each of the specific security recommendations as we develop the program.