OLA **OFFICE OF THE LEGISLATIVE AUDITOR**
**STATE OF MINNESOTA**

**FINANCIAL AUDIT DIVISION REPORT**

# Minnesota State Retirement System

## Information Technology Audit

**June 23, 2009** **Report 09-23**

FINANCIAL AUDIT DIVISION
Centennial Building – Suite 140
658 Cedar Street – Saint Paul, MN 55155
Telephone: 651-296-4708 • Fax: 651-296-4712
E-mail: auditor@state.mn.us • Web site: http://www.auditor.leg.state.mn.us
Through Minnesota Relay: 1-800-627-3529 or 7-1-1

OLA

**OFFICE OF THE LEGISLATIVE AUDITOR**

**State of Minnesota • James Nobles, Legislative Auditor**

June 23, 2009

Senator Ann H. Rest, Chair
Legislative Audit Commission

Members of the Legislative Audit Commission

Mr. Dave Bergstrom, Executive Director
Minnesota State Retirement System

This report presents the results of our information technology audit of the Minnesota State Retirement System's (MSRS) controls. The scope of our audit focused on controls that help to protect the integrity, confidentiality, and availability of MSRS's computer systems and business data. This report contains eight findings presented in the accompanying section of this report titled, *Findings and Recommendations*.

We discussed the results of the audit with MSRS's staff on June 11, 2009. Management's response to our findings and recommendations are presented in the accompanying section of this report titled, *Agency Response.*

The audit was conducted by Eric Wion (Audit Manager) and Aimee Martin (Auditor-in-Charge), assisted by auditors John Kelcher and Bill Betthauser.

| | |
|---|---|
| */s/ James R. Nobles* | */s/ Cecile M. Ferkul* |
| James R. Nobles<br>Legislative Auditor | Cecile M. Ferkul, CPA, CISA<br>Deputy Legislative Auditor |

# Table of Contents

# Report Summary

## Conclusion

The Minnesota State Retirement System (MSRS) did not have adequate controls to protect the integrity, confidentiality, and availability of its computer systems and business data. Serious security weaknesses exposed them to an unacceptable risk of tampering, disclosure, and disruption. The report contains eight findings relating to internal control deficiencies.

## Findings

- MSRS did not have a comprehensive security management program. (Finding 1, page 5)
- Poor firewall and wireless security controls exposed MSRS's private internal network to external threats. (Finding 2, page 6)
- MSRS did not sufficiently segment its internal private network to improve security over its computer systems and data. (Finding 3, page 7)
- MSRS did not monitor security-related events. (Finding 4, page 7)
- MSRS did not have strong account and password controls. (Finding 5, page 8)
- MSRS did not adequately restrict employee access to some computer systems and data, and it did not encrypt sensitive data. (Finding 6, page 9)
- MSRS did not follow adequate change management procedures. (Finding 7, page 10)
- MSRS did not promptly install software updates or security-related software patches on some of its computers, and some were running unnecessary and insecure software. (Finding 8, page 10)

## Audit Objective and Scope

The audit objective was to answer the following question:

- Did MSRS have adequate controls to protect the integrity, confidentiality, and availability of its computer systems and business data?

We assessed controls as of April 2009.

## Background

MSRS administers six retirement plans, a supplemental retirement plan for Hennepin County, and health care and deferred compensation plans for state employees and other public employees.  Plan membership is comprised of state employees, state law enforcement and correctional officers, constitutional officers, legislators, judges, employees of the University of Minnesota, the Metropolitan Council, and employees of various other designated public agencies. Approximately 700 employers participate in the plans whose membership includes over 250,000 active and inactive employees and their beneficiaries.

# Minnesota State Retirement System

## Agency Overview

The Minnesota State Retirement System (MSRS) administers six defined benefit retirement plans: the State Employees Plan, State Patrol Plan, Correctional Employees Plan, Judges Plan, Legislators Plan, and the Elective State Officers Plan. It also administers four defined contribution plans: the Unclassified Employees Plan, Hennepin County Supplemental Retirement Plan, Health Care Savings Plan, and the Minnesota State Deferred Compensation Plan. Public employees and sometimes their employers contribute to these plans during their working years and obtain benefits upon retirement, disability, or termination of employment.

Approximately 700 government employers and over 250,000 active and inactive employees and their beneficiaries participated in the plans.[1] At June 30, 2008, MSRS reported that its pension funds had $14.4 billion in net assets. Fiscal year 2008 plan contributions and payments were $572 million and $766 million, respectively.[2]

MSRS developed the computer systems used to manage the majority of its day-to-day business operations. These systems reside at the Office of Enterprise Technology (OET). MSRS and OET jointly share responsibility for the management of these systems. MSRS also manages its own private internal network consisting of many network devices, desktop computers, and servers. Employees use computers on its private internal network to access the computer systems at OET.

## Objective, Scope, and Methodology

The audit objective was to answer the following question:

- Did MSRS have adequate controls to protect the integrity, confidentiality, and availability of its computer systems and business data?

To answer this question, we interviewed MSRS and OET staff and reviewed policies, procedures, and other relevant documentation. We also used a variety of

[1] 2010-11 Biennial Budget.
[2] MSRS 2008 Comprehensive Annual Financial Report.

computer-assisted auditing tools and other techniques to analyze the security infrastructure.

We conducted this audit in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. To assess security controls, we used criteria contained in the *Control Objectives for Information and Related Technology (COBIT*),[3] published by the IT Governance Institute. We also used criteria obtained in security guidance published by the National Institute of Standards and Technology's Computer Security Division, the National Security Agency, and the Defense Information Systems Agency. Finally, we used information published by applicable technology vendors to evaluate select controls.

# Conclusion

MSRS did not have adequate controls to protect the integrity, confidentiality, and availability of its computer systems and business data. Serious security weaknesses exposed them to an unacceptable risk of tampering, disclosure, and disruption. The following *Findings and Recommendations* section explains the deficiencies.

[3] COBIT is an IT governance framework providing organizations with a set of generally accepted measures, indicators, processes, and best practices to assist them in developing appropriate IT governance and control in an organization.

# Findings and Recommendations

## Finding 1

**MSRS did not have a comprehensive security management program.**

MSRS did not have a comprehensive security management program that was capable of responding promptly to constantly changing technology risks. A security management program is a formal way to manage risks effectively throughout the organization and promptly respond to constantly changing threats. Not unlike other important business functions, such as accounting and finance, responsibility and authority for security should be established at the highest levels of the organization, be well managed, and include appropriate planning and oversight.

MSRS did not define the security program's scope, objectives, goals, and responsibilities. In April 2008, MSRS hired an employee whose primary responsibility was to establish and monitor a security management program. However, the employee had to focus primarily on mitigating a large number of security vulnerabilities and has had little time to develop the security management program.

MSRS had not developed risk assessment methodologies nor conducted a risk assessment. Without an assessment of risks, MSRS's management did not know the degree of risk that existed nor could it determine what level of risk was acceptable and what steps it needed to take to reach that level. The results of this analysis also would help MSRS design policies, standards, and procedures to reduce its exposure to a level that management is willing to accept.

MSRS did not have written policies, standards, or procedures addressing information technology risks and security. These are critical because they outline management's security expectations and methods to fulfill those expectations. Employees cannot make consistent security decisions without policies and standards to refer to as guidance.

*Recommendation*

- *MSRS should develop a comprehensive security management program.*
  - *It should define the program's scope, objectives, goals, and responsibilities.*
  - *It should develop risk assessment methodologies and perform periodic assessments.*
  - *It should develop written security policies, standards, and procedures and monitor compliance with them.*

## Finding 2

**Poor firewall and wireless security controls exposed MSRS's private internal network to external threats.**

MSRS poorly configured, managed, documented, and understood its firewall and wireless technologies. As a result, significant control deficiencies existed that exposed their private internal network to external threats that included the distribution of malicious software and unauthorized access.

A firewall is typically an organization's first line of defense against external threats from hackers. A firewall is a computer that separates an organization's private internal network from the public Internet. Serving as gatekeeper, a firewall examines all traffic that attempts to enter or leave an organization's private network. Traffic that does not meet certain conditions, defined in firewall rules, cannot pass in or out of the private network.

MSRS's firewall rules did not adequately protect computers on the internal network. MSRS also had some computers that were not behind the firewall. As a result, the firewall could not protect them. These weaknesses were significant because hackers on the Internet could easily detect and exploit them with automated tools to gain unauthorized access to the private network.

MSRS connected several poorly secured wireless access points to its private internal network to provide a few employees with wireless telephones. These weaknesses were significant because hackers could easily detect and exploit them with automated tools to bypass the firewall and gain unauthorized access to its private internal network. MSRS took swift action and disconnected the wireless devices after we told employees about the security risks.

### *Recommendations*

- *MSRS should protect all computers with its firewall.*
- *MSRS should establish firewall rules to restrict inbound and outbound Internet traffic to the minimum needed to conduct business.*
- *MSRS should determine whether employees need additional training to adequately understand and secure the private internal network.*

## Finding 3

**MSRS did not sufficiently segment its internal private network to improve security over its computer systems and data.**

MSRS did not sufficiently segment its internal private network to filter computer traffic and improve security. Internal network segmentation improves control by only allowing authorized traffic in or out of each segment on the private internal network. For example, an organization may place workstation or laptop computers used by business employees in a different segment than a computer running business software or containing sensitive data. Without this segmentation, someone who gained unauthorized access to MSRS's private internal network could freely move throughout the network and attempt to access any computer and software on them. For example, anyone could attempt to access powerful programs that only information technology employees need to access. Segmentation also helps prevent the spread of malicious software, such as viruses, worms, and trojans.

*Recommendation*

- *MSRS should further segment its internal network and only allow authorized traffic between each segment.*

## Finding 4

**MSRS did not monitor security-related events.**

MSRS did not have monitoring procedures to detect and promptly respond to security-related events. In addition to external attacks such as unauthorized attempts to access computers, other events require monitoring, such as system misuse by employees, changes to critical computer settings, and exceptions to defined policies and procedures.

MSRS did not assess its risks and define specific events to log, who should review them, and the frequency of the review. In most cases, MSRS did not log or monitor security events. Manual procedures alone will never be effective because the variety and number of computers and the volume of security events make monitoring a very daunting task. Organizations need software to assist in the gathering and analyzing of security logs to identify events that require attention. All computers, including very critical ones, such as the firewall, include software that MSRS could customize to log various types of security events.

Although the best security controls are those that prevent inappropriate events from happening, it is virtually impossible to design flawless preventive defenses. This inherent security administration problem is why every organization must vigilantly monitor its systems for signs of attack or abuse.

*Recommendation*

- *MSRS should define specific events to log, who should review them, and the frequency of the review.*

## Finding 5

**MSRS did not have strong account and password controls.**

MSRS did not configure some computers and computer programs to enforce strong password controls. Strong password controls are critical because they help prevent hackers from assuming the identity of legitimate system users. Most computer systems have customizable features to enforce strong password controls. For example, features can prevent users from selecting easy to guess passwords, like dictionary words, and require that employees periodically change their passwords. We examined these and other customizable password features and found several inconsistencies and weaknesses.

Some accounts, including very powerful administrator accounts, had weak, easily guessable passwords. In addition, MSRS had not changed the password for one powerful account from the default given by the software vendor. Many purchased software products come with default user accounts and passwords. Hackers often use this knowledge to gain unauthorized access, and several websites on the Internet contain lists of default accounts and passwords for most purchased software products.

Finally, some staff shared accounts and passwords with extremely powerful security clearances. Sharing passwords is never acceptable because it eliminates individual accountability. Information security relies on two fundamental principles: 1) positively confirming the identity of system users and 2) always having a mechanism to trace critical activities to specific individuals. Choosing not to strongly enforce these principles exposed the computer systems and their data to unnecessary risks.

*Recommendations*

- *MSRS should implement and enforce strong account and password controls.*
- *MSRS should promptly change all default and easy to guess passwords.*
- *MSRS should prohibit the sharing of accounts and passwords.*

## Finding 6

**MSRS did not adequately restrict employee access to some computer systems and data, and it did not encrypt sensitive data.**

MSRS did not have adequate controls to ensure it provided employees with appropriate access to critical resources, such as its business applications and sensitive data. In addition, it did not encrypt sensitive, not public data.

Some MSRS employees had inappropriate access to the computer application used to manage retirement accounts and other information. For example:

- Five people had the ability to modify employees' security clearances.
- Five information technology staff, including two computer programmers, had the ability to use the application to enter business transactions.

Some MSRS and non-MSRS employees had inappropriate access to the database, which stored retirement account data and other electronic files. For example:

- Five people had unnecessary system administrator access.
- Six people, including three computer programmers, had powerful access, including the ability to read and modify any data in the database.
- Many people had the ability to read electronic files, including files containing not public data.

MSRS did not encrypt sensitive, not public data during transmission and storage. For example, employers transmitted unencrypted, not public employee data, including personal and financial information, to MSRS. Finally, MSRS did not encrypt data, including member passwords, security answers, social security numbers, and bank account numbers stored in its database. Encryption converts data into a format that is unreadable and is an important control to help protect sensitive data from unauthorized disclosure.

### *Recommendations*

- *MSRS should restrict access to computer systems and data to only those who have a business need.*
- *MSRS should develop procedures to periodically review and recertify computer users' access.*
- *MSRS should encrypt sensitive, not public data during transmission and storage.*

## Finding 7

**MSRS did not follow adequate change management procedures.**

Change management is a process of managing and controlling all changes to the technology infrastructure. Its purpose is to implement only appropriate and authorized changes, causing minimal disruption. Changes often are frequent and can take many forms, including changes to processes, computer programs, and computer settings.

Computer programmers performed or had the ability to perform incompatible duties, including developing, testing, and migrating computer programs. Separating duties is a fundamental change management control. Also, MSRS did not consistently document computer program changes, including requests, business requirements, testing procedures and results, or formal approvals.

Other changes to technology infrastructure did not typically follow a standard change management process. Examples of these changes include software patches or updates and computer configuration changes, including security-related changes.

Failure to follow stringent change management procedures may result in unauthorized changes, computer disruption, or security vulnerabilities.

*Recommendations*

- *MSRS should ensure that all computer-related changes follow stringent change management procedures.*

- *MSRS should separate incompatible duties performed by computer programmers.*

## Finding 8

**MSRS did not promptly install software updates or security-related software patches on some of its computers, and some were running unnecessary and insecure software.**

Computer hackers routinely discover and exploit flaws in commercial software to gain unauthorized access to computer systems. When these exploits occur, vendors develop and publish software patches to correct the deficiencies in their products. Agencies that do not promptly install these software patches make their systems easy targets for computer hackers. Staying up to date with software patches can be a very challenging task for an organization. To meet this challenge, organizations need a formal process to learn about new vulnerabilities and determine whether their systems are at risk. In addition, organizations need formal testing and installation procedures that include an exit strategy, should a software patch result in a system failure.

Some of MSRS's computers were running unnecessary and insecure software. We identified some software on computers that were not necessary. In several cases, the software was susceptible to common hacker exploits.

*Recommendation*

- *MSRS should regularly install software patches and limit software to those that are authorized, necessary, and secure.*

MSRS | Minnesota State Retirement System
MNDCP | Minnesota Deferred Compensation Plan
HCSP | Health Care Savings Plan

June 18, 2009

James R. Nobles, Legislative Auditor
Office of the Legislative Auditor
Room 140 Centennial Building
658 Cedar Street
St. Paul, MN 55155-1603

Dear Mr. Nobles:

We appreciate the opportunity to review and respond to your first audit of the Minnesota State Retirement System's information technology (IT) security controls. We also want to thank your IT audit team for their fine work on this engagement.

Overall, we find your conclusion to be a fair assessment. However, we would like to emphasize that our sensitive member data and mission-critical applications reside securely on the Office of Enterprise Technology's (OET) mainframe computers. While our network provides less sensitive support functions for staff, it does provide opportunities that expose some private data to external threats. To the best of our knowledge, no personal identifying data has been compromised.

The results of your audit complement the strategic and tactical recommendations which emerged from penetration tests that OET staff conducted about two years ago. At that time, we made a commitment to improve our security posture, which included the hiring of a full-time systems security engineer. We believe that we've made good progress, especially within the past year, to enhance our security controls. Yet we realize that we have considerable work to do to get to where we would like our IT security environment to be.

We recognize the importance of strong IT controls. As always, we take our responsibility for security controls and your findings very seriously. We intend to take the necessary remedial actions to implement your recommendations and resolve the audit issues contained in this report.

**Finding 1. MSRS did not have a comprehensive security management program.**

*Recommendation*

1. *MSRS should develop a comprehensive security management program.*

- *It should define the program's scope, objectives, goals, and responsibilities.*

- *It should develop risk assessment methodologies and perform periodic assessments.*

- *It should develop written security policies, standards, and procedures and monitor compliance with them.*

*MSRS Response:*

We expected that this finding and recommendation would be a report comment prior to the commencement of the IT security audit. In June, 2007 we worked with OET to conduct penetration tests to identify any system vulnerabilities. After we received the penetration testing results in October, 2007 we recognized that we need (1) to mitigate known vulnerabilities identified in the testing and (2) to develop, implement, and maintain a comprehensive security management plan designed to protect the confidentiality, integrity and availability of all MSRS information systems and data. Our priority focused on vulnerability management over the development of the comprehensive security management plan.

With the deployment of OET's Enterprise Vulnerability Management System in July 2008, we've been able to track our progress in managing vulnerabilities. We've seen dramatic reductions in our vulnerability count and their severity level. New MSRS policies, standards and procedures are evolving from our vulnerability remediation efforts; they will be components of our comprehensive security management plan. Development, implementation, and maintenance of this plan will be an ongoing project.

*Persons responsible:*
Judy Hunt, Assistant Executive Director
Al Cooley, Information Systems Manager
Bart Wallace, Systems Security Engineer

*Target date for resolution of the finding:*
June 30, 2011 for the framework of the comprehensive security management plan and development of a core group of security policies

**Finding 2. Poor firewall and wireless security controls exposed MSRS' private internal network to external threats.**

*Recommendations*

2. *MSRS should protect all computers with its firewall.*

3. *MSRS should establish firewall rules to restrict inbound and outbound Internet traffic to the minimum needed to conduct business.*

4. *MSRS should determine whether employees need additional training to adequately understand and secure the private internal network.*

*MSRS Response:*

We agree with the finding and your recommendations and have implemented stronger controls to improve the security of our internal network. We moved all of our most vulnerable devices behind our firewall, and have another device which will be moved by the end of July. We also have revised our firewall rules based on your recommendations. We currently are evaluating these rules to see where additional changes may be necessary. We intend to develop a process for approving and monitoring changes to our firewall rules before calendar year end. We recognize the importance of technical training for staff and sent five of our staff to a total of eight security-related training opportunities last year. We anticipate expanding the scope of our security training to staff in fiscal year 2010.

*Person responsible:* Al Cooley, Information Systems Manager

*Target dates for resolution of the finding:*
Recommendation 2 – July 31, 2009
Recommendation 3 – December 31, 2009
Recommendation 4 – June 30, 2010

**Finding 3. MSRS did not sufficiently segment its internal private network to improve the security over its computer systems and data.**

*Recommendation*

5. *MSRS should further segment its internal network and only allow authorized traffic between each segment.*

*MSRS Response:*

We agree with the finding and the recommendation. During fiscal year 2010, we will begin a multi-phased project aimed at redesigning our network architecture with an emphasis on security and the ability to enhance our security controls. As part of this project, we will explore ways to filter and segment traffic internally and give consideration to having additional firewalls and virtual local area networks.

*Person responsible:* Bart Wallace, Systems Security Engineer

*Target date for resolution of the finding:* June 30, 2010

**Finding 4. MSRS did not monitor security-related events.**

*Recommendation*

6. *MSRS should define specific events to log, who should review them, and the frequency of the review.*

*MSRS Response:*

We concur with the finding and the recommendation. We are in the process of making it easier to identify and review security events. We will be implementing policies, standards, and procedures for logging and conducting event reviews based on decisions made in the development of our comprehensive security management plan.

*Person responsible:* Bart Wallace, Systems Security Engineer

*Target date for resolution of the finding:* June 30, 2011

**Finding 5. MSRS did not have strong account and password controls.**

*Recommendations*

7. *MSRS should implement and enforce strong account and password controls.*

8. *MSRS should promptly change all default and easy to guess passwords.*

9. *MSRS should prohibit the sharing of accounts and passwords.*

*MSRS Response:*

We agree with the finding and the recommendations. We recently implemented a network device password policy and have changed many easy to guess passwords. This is a first step in our development of stronger account and password controls. We will also create individual accounts necessary to prevent future sharing of passwords.

*Person responsible:* Al Cooley, Information Systems Manager

*Target dates for resolution of the finding:*
Recommendation 7 – June 30, 2010
Recommendation 8 – Already implemented.
Recommendation 9 – December 31, 2009

**Finding 6. MSRS did not adequately restrict employee access to some computer systems and data, and it did not encrypt sensitive data.**

*Recommendations*

10. *MSRS should restrict access to computer systems and data to only those who have a business need.*
11. *MSRS should develop procedures to periodically review and recertify computer users' access.*
12. *MSRS should encrypt sensitive, not public data during transmission and storage.*

*MSRS Response:*

We concur with th e finding and the recommendations. W e will work with OE T staff to restrict employees' access to files containing sensitive data. We will also explore other options to help secure or encrypt sensitive data.

*Person responsible:* Al Cooley, Information Systems Manager

*Target dates for resolution of the finding:*
Recommendation 10 – December 31, 2009
Recommendation 11 – December 31, 2009
Recommendation 12 – June 30, 2010

**Finding 7. MSRS did not follow adequate change management procedures.**

*Recommendations*

13. *MSRS should ensure that all computer-related changes follow stringent change management procedures.*

14. *MSRS should separate incompatible duties performed by computer programmers.*

*MSRS Response:*

Similar to finding 1, we knew that this weakness would surface as an audit issue. We recognize the importance of change management as the foundation for a stronger IT environment. We are currently developing a change management process. To fully resolve this audit issue, we will need to work with OET staff to have them establish the libraries and controls necessary to facilitate the change management process.

*Person responsible:* Al Cooley, Information Systems Manager

*Target dates for resolution of the finding:*
Recommendation 13 – June 30, 2010
Recommendation 14 – June 30, 2010

**Finding 8. MSRS did not promptly install software updates or security-related software patches on some of its computers, and some were running unnecessary and insecure software.**

*Recommendation*

*15. MSRS should regularly install software patches and limit software to those that are authorized, necessary, and secure.*

*MSRS Response:*

We also agree with this finding and recommendation. We intend to develop a patch management process, complete with detailed policies and procedures. This process will focus on installing software patches on higher priority or critical devices first, and having the installations complete within a reasonable time of their release. We will also develop policies, standards, and procedures to prevent the future use of insecure software.

*Person responsible:* Al Cooley, Information Systems Manager

*Target date for resolution of the finding:* June 20, 2010

Again, we appreciate the opportunity to respond to the report comments. We value the work of your IT audit team for identifying the most significant technical vulnerabilities that expose our systems and data to external threats, and offering practical recommendations to mitigate those vulnerabilities. We are committed to taking appropriate actions to further improve our security posture and internal control structure.

Sincerely,

David Bergstrom

David Bergstrom
Executive Director

cc: Al Cooley Judy Hunt Erin Leonard Bart Wallace