OLA
OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA

FINANCIAL AUDIT DIVISION REPORT

Department of Administration

Information Technology Audit

As of September 2010

November 4, 2010 **Report 10-35**

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

November 4, 2010

Senator Ann H. Rest, Chair
Legislative Audit Commission

Members of the Legislative Audit Commission

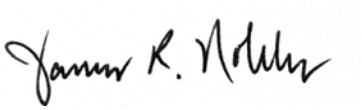
Ms. Sheila Reger, Commissioner
Minnesota Department of Administration

This report presents the results of our audit of the Department of Administration's security controls that help to protect the department's computer systems and data from external threats. This report contains five findings presented in the accompanying section of this report titled, *Findings and Recommendations*.

We discussed the results of the audit with the department's staff on October 25, 2010. Management's response to our findings and recommendations is presented in the accompanying section of this report titled, *Agency Response*.

The audit was conducted by Eric Wion, CPA, CISA (Audit Manager), Aimee Martin, CISA (Auditor-in-Charge), Carolyn Engstrom, CISA (Audit Coordinator), and Bill Betthauser, CISA (Senior Auditor).

This report is intended for the information and use of the Legislative Audit Commission and the management of the Department of Administration. This restriction is not intended to limit the distribution of this report, which was released as a public document on November 4, 2010.



James R. Nobles
Legislative Auditor

Cecile M. Ferkul, CPA, CISA
Deputy Legislative Auditor

Room 140 Centennial Building, 658 Cedar Street, St. Paul, Minnesota 55155-1603 • Tel: 651-296-4708 • Fax: 651-296-4712
E-mail: auditor@state.mn.us • Web Site: www.auditor.leg.state.mn.us • Through Minnesota Relay: 1-800-627-3529 or 7-1-1

Table of Contents

Report Summary

Conclusion

The Department of Administration generally had adequate security controls to protect the confidentiality, integrity, and availability of its data and computer systems from threats originating outside its internal network. However, we identified five weaknesses in internal controls.

Findings

- The Department of Administration had not adequately managed its information security risks and lacked some written agreements with the Office of Enterprise Technology. (Finding 1, page 5)

- The Department of Administration had not adequately assessed, prioritized, reported, and remediated vulnerabilities. (Finding 2, page 6)

- The Department of Administration had not assessed its monitoring needs nor did it proactively review security events. (Finding 3, page 7)

- The Department of Administration lacked change control procedures for its firewall rules. (Finding 4, page 7)

- The Department of Administration had not periodically recertified some access privileges, and some information technology staff shared passwords. (Finding 5, page 8)

Audit Objective and Scope

The audit objective was to answer the following question:

- Did the Department of Administration have adequate security controls to protect the department's computer systems and data from external threats?

We assessed controls as of September 2010.

Department of Administration

Information Technology Security Controls

Overview

The Department of Administration provides a broad range of business management, administrative and professional services, and a variety of resources to state and local government agencies and to the public. During fiscal year 2009, the department had approximately 500 employees and spent over $170 million derived from various funding sources.[1]

As of September 2010, the department had a decentralized information technology structure with information technology staff spread across business divisions that were responsible for the day-to-day management of computer systems. The department's part-time chief information officer, available through an interagency agreement with the Office of Enterprise Technology, was responsible for developing the department's overall information technology strategies and plans.[2] The department also had an interagency agreement with the Office of Enterprise Technology to manage many aspects of the department's computing environment, including its network and select computers.

Objective, Scope, and Methodology

Our audit objective was to answer the following question:

- Did the Department of Administration have adequate security controls to protect the confidentiality, integrity, and availability of its data and computer systems from external threats?

To answer this question, we interviewed staff at the department and the Office of Enterprise Technology and reviewed relevant documentation. We also used a variety of computer-assisted auditing tools and other techniques to analyze the security infrastructure and test controls. We assessed controls as of September 2010.

[1] State of Minnesota Biennial Budget 2010-11.

[2] The employee in the Department of Administration's chief information officer position allocates about 20 percent of his time to the Department of Administration and 80 percent of his time to information technology duties at the Office of Enterprise Technology.

The audit focused on the department's controls that protect its data from unauthorized disclosure and modification resulting from external threats, such as hackers, or threats that result from internal users accessing external malicious resources. Organizations often implement controls at multiple layers of a computer network so that if one control fails, other controls will mitigate the risk of compromise. Examples of controls reviewed include network design, firewall and network device management, remote access, patch management, anti-virus software scanning, and vulnerability and threat management.

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 *Special Publication 800-53, Recommended Security Controls for Federal Information Systems*, published by the National Institute of Standards and Technology's Computer Security Division. We also used criteria contained in security guidance, published by the Defense Information Systems Agency, and information published by applicable technology vendors to evaluate select controls. When available, we also used department and state policies to obtain evaluation criteria.

Conclusion

The Department of Administration generally had adequate security controls to protect the confidentiality, integrity, and availability of its data and computer systems from external threats. However, the department had some weaknesses in its internal controls.

The following *Findings and Recommendations* section explains the weaknesses.

Findings and Recommendations

Finding 1

The Department of Administration had not adequately managed its information security risks and lacked some written agreements with the Office of Enterprise Technology.

The department had not adequately managed its information security risks. Of most significance, the department had not designated a specific person, such as a chief information security officer, with responsibility and authority to develop and enforce a security program. Instead, management relied on information technology staff, spread across several business units, to make security decisions and implement controls, without providing them appropriate oversight to ensure consistent and appropriate practices. Information technology staff's position descriptions did not define specific security-related roles and responsibilities. Without clear documentation of these roles and responsibilities, the department's information technology staff typically allowed daily operational duties to take priority over security practices. Since technology and risks are constantly changing, it is critical that the department have staff whose primary job responsibilities are to manage its security program.

In addition, the department did not sufficiently assess the risks associated with various technology changes to ensure the department implemented appropriate security controls. For example, the department was unaware that information technology staff in one of its business units had installed an insecure wireless access device. Had the department assessed the risk associated with the insecure wireless device, it likely would have not allowed the business unit to install it. The department removed the device based on information provided through our audit.

In addition, the department did not have service level agreements for key services it obtained from the Office of Enterprise Technology. These key services included critical security-related processes, such as managing firewall rules and patching computer software that have known vulnerabilities. Service level agreements are negotiated, formal agreements that stipulate the provided services, priorities, responsibilities, including security-related requirements, guarantees, and warranties. Without developing and monitoring formal agreements, the department cannot ensure that the Office of Enterprise Technology has met the department's security requirements.

Recommendations

- *The department should give a person or group the responsibility and authority to develop, implement, and monitor the effectiveness of the security program.*

- *The department should define the program's scope, objectives, goals, and responsibilities, including the roles and responsibilities of individuals and groups that play a vital role in security.*

- *The department should require and monitor service level agreements with the Office of Enterprise Technology.*

Finding 2

The Department of Administration had not adequately assessed, prioritized, reported, and remediated vulnerabilities.

The department had not developed formal procedures to assess, prioritize, report, and remediate vulnerabilities identified through its routine computer scans using the state's Enterprise Vulnerability Management System. The department's scans identified several computers, including those managed by the Office of Enterprise Technology, with high vulnerability scores. A high score indicates that the computer is vulnerable because of a variety of factors, including the severity of weaknesses created by not applying available software upgrades and patches.

Vulnerability management software can produce a large volume of data. Without formal procedures, the department may not notice or resolve critical vulnerabilities in a timely manner. The department could have resolved many of the vulnerabilities by installing software patches or updates.

Agencies that do not promptly fix critical vulnerabilities make their systems easy targets for computer hackers. State policy requires each agency to manage and monitor their computers for vulnerabilities and implement and maintain vulnerability remediation processes.[3]

Recommendation

- *The department should develop a formal vulnerability and threat management program to ensure it, and the Office of Enterprise Technology, corrects or mitigates critical vulnerabilities in a timely manner.*

[3] Office of Enterprise Technology: *Enterprise Security Technical Control Policies 2010-02, TC01 – Vulnerability and Threat Management Policy.*

Finding 3

The Department of Administration had not assessed its monitoring needs nor did it proactively review security events.

The department did not have sufficient monitoring procedures to detect and appropriately respond to important security-related events, such as potential external attacks, unauthorized attempts to access computers or sensitive files, changes to critical computer settings, employee system misuse, and exceptions to defined policies and procedures in a timely manner. The department had weaknesses in the following areas:

- The department had not assessed which security-related events, including those on computers managed by the Office of Enterprise Technology, put its systems and data at highest risk.

- The department did not regularly review any of its security logs. It had not assigned the review of the logs to specific staff, identified how frequently to review logs, or prescribed the action staff should take in response to suspicious activity.

- The department did not develop and implement a strategy to ensure it maintained, backed up, and archived all security log records. It is important to have historic log information available should the department or law enforcement need to conduct an investigation.

Without adequate security event monitoring procedures, it is unlikely that the department would take prompt and appropriate action to protect its computer systems and data if an attack occurred.

Recommendations

- *The department should assess its monitoring needs to determine what events it needs to log, who should review the logs, and the frequency of the review. It should consider automating the systematic review and analysis of security events.*
- *The department should define and follow its records retention requirements for security log records.*

Finding 4

The Department of Administration lacked change control procedures for its firewall rules.

The Department of Administration lacked change control procedures for its firewall rules, including procedures to request, review, approve, and document the changes. The department had not identified an independent person, such as a

security specialist, to review, assess, and approve rule requests. In addition, the department had not periodically reviewed and recertified the existing rules to ensure they were appropriate.

The Office of Enterprise Technology provided the department with firewall services; at the department's request, the office created and modified firewall rules that allowed or prohibited computer traffic into or out of the department's private network. However, the Office of Enterprise Technology lacked processes to periodically review and recertify firewall rules, although an internal audit or assessment conducted by the office's Enterprise Security Office identified this weakness in June 2008.

Recommendation

- *The Department of Administration should work with the Office of Enterprise Technology to develop formal procedures for firewall rule changes, including procedures to request, review, approve, and document the changes. Procedures should also include the periodic review and recertification of the firewall rules.*

Finding 5

The Department of Administration had not periodically recertified some access privileges, and some information technology staff shared passwords.

The department did not periodically review and reconfirm the need for some employees to access critical devices or remotely access the department's private internal network from outside the network. The department's failure to periodically review employees' access could result in current or former employees having access they no longer need.

Some information technology staff shared passwords used to administer or manage critical devices. Sharing passwords prevents the department from determining employee accountability for changes made to its computer systems.

Recommendations

- *The department should periodically review and recertify those with network device and remote access to ensure that they still require access.*

- *The department should prohibit the sharing of passwords.*

November 1, 2010

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

Dear Mr. Nobles:

The professional review and assessment of the Office of Legislative Auditor (OLA) team has provided an opportunity to assess both the strengths and weaknesses of information security practices at the Department of Administration. We greatly appreciate the work of the OLA team, agree with its findings, and already have put into motion strategies that will address risks in the department.

We are pleased with the audit's conclusion that the Department of Administration "generally had adequate security controls" in place. As a functionally diverse agency that deploys a wide variety of technologies in support of its programs, we believe that this demonstrates our commitment and technical capacity to provide a high level of security. We will build on this solid framework to address the OLA audit's findings.

Finding 1: The Department of Administration had not adequately managed its information security risks and lacked some written agreements with the Office of Enterprise Technology (OET).

Recommendations

- *The department should give a person or group the responsibility and authority to develop, implement, and monitor the effectiveness of the security program.*

- *The department should define the program's scope, objectives, goals, and responsibilities, including the roles and responsibilities of individuals and groups that play a vital role in security.*

- *The department should require and monitor service level agreements with the Office of Enterprise Technology.*

Response: The department agrees with the finding and has initiated actions to ensure a comprehensive security management program is in place. A Chief Information Security Officer (CISO) will be identified by March 1, 2011. The CISO will develop the program including provisions for monitoring its effectiveness. The program will be based on policies, standards and guidelines specified by the Enterprise Security Program adopted by OET's Security Management Office. The comprehensive security management program plan will be in place by May 31, 2011.

The department will work with OET to develop Service Level Agreements (SLAs), focusing first on IT security services, but also examining other OET delivered services. The CIO and the CISO will be responsible for this task and will have the IT Security SLAs in place by May 31, 2011.

Finding 2: The Department of Administration had not adequately assessed, prioritized, reported and remediated vulnerabilities.

Recommendation

- *The department should develop a formal vulnerability and threat management program to ensure it, and the Office of Enterprise Technology, corrects or mitigates critical vulnerabilities in a timely manner.*

Response: The department agrees with this finding and recommendation. Admin will develop a formal vulnerability and threat management plan by May 31, 2011 that will include an assessment of risks, identification of priorities and a protocol for reporting and remediating vulnerabilities. The CISO will be responsible for developing and implementing the plan.

Finding 3: The Department of Administration had not assessed its monitoring needs nor did it proactively review security events.

Recommendations

- *The department should assess its monitoring needs to determine what events it needs to log, who should review the logs, and the frequency of the review. It should consider automating the systematic review and analysis of security events.*
- *The department should define and follow its records retention requirements for security log records.*

Response: The department agrees with this finding and the recommendations. The department periodically assesses its monitoring needs, but will ensure future assessments are more comprehensive and include a systematic monitoring program. Admin will develop and implement a formal security event monitoring program by May 31, 2011. The program will comply with guidelines established by OET and will comply with the state's records retention requirements for security log records. The CISO will be responsible for preparing the plan and implementing the program.

Finding 4: The Department of Administration lacked change control procedures for its firewall rules.

Recommendation

- *The Department of Administration should work with the Office of Enterprise Technology to develop formal procedures for firewall rule changes, including procedures to request, review, approve, and document the changes. Procedures should also include the periodic review and recertification of the firewall rules.*

Response: The department agrees with the recommendation. Firewall rules for the department are administered by OET, which also maintains the change control procedures that Admin follows. The department agrees that firewall change control procedures should be improved and will work with OET to develop and implement formal procedures. These procedures will include periodic review and recertification. The CISO will be responsible for this activity.

Finding 5: The Department of Administration had not periodically recertified some access privileges, and some information technology staff shared passwords.

Recommendations

- *The department should periodically review and recertify those with network device and remote access to ensure that they still require access.*

- *The department should prohibit the sharing of passwords.*

Response: The department agrees with the finding and recommendations and will develop and implement policies and procedures to periodically review and certify access privileges and password controls and to prohibit sharing of passwords. The CIO and CISO will be responsible for developing this plan by June 30, 2011.

Sincerely,

Sheila M. Reger
Commissioner