OLA OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA

FINANCIAL AUDIT DIVISION REPORT

Department of Education

Network Security Controls

Information Technology Audit

May 5, 2010 **Report 10-17**

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

Financial Audit Division

The Financial Audit Division annually audits the state's financial statements and, on a rotating schedule, audits agencies in the executive and judicial branches of state government, three metropolitan agencies, and several "semi-state" organizations. The division has a staff of forty auditors, most of whom are CPAs. The division conducts audits in accordance with standards established by the American Institute of Certified Public Accountants and the Comptroller General of the United States.

The Office of the Legislative Auditor (OLA) also has a Program Evaluation Division, which evaluates topics periodically selected by the Legislative Audit Commission.

Reports issued by both OLA divisions are solely the responsibility of OLA and may not reflect the views of the Legislative Audit Commission, its individual members, or other members of the Minnesota Legislature. For more information about OLA reports, go to:

http://www.auditor.leg.state.mn.us

To obtain reports in electronic ASCII text, Braille, large print, or audio, call 651-296-4708. People with hearing or speech disabilities may call through Minnesota Relay by dialing 7-1-1 or 1-800-627-3529.

To offer comments about our work or suggest an audit, investigation, or evaluation, call 651-296-4708 or e-mail auditor@state.mn.us.

O L A **OFFICE OF THE LEGISLATIVE AUDITOR**

State of Minnesota • James Nobles, Legislative Auditor

May 5, 2010

Senator Ann H. Rest, Chair
Legislative Audit Commission

Members of the Legislative Audit Commission

Ms. Alice Seagren, Commissioner
Minnesota Department of Education

This report presents the results of our audit of the Department of Education's security controls that help to protect the department's computer systems and data from external threats. This report contains six 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 April 26, 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 (Audit Manager), Carolyn Engstrom (Auditor-in-Charge), Aimee Martin (Senior Auditor), and Bill Betthauser (Senior Auditor).

James R. Nobles | Cecile M. Ferkul

James R. Nobles
Legislative Auditor

Cecile M. Ferkul, CPA
Deputy Legislative Auditor

Table of Contents

Report Summary

Conclusion

The Department of Education did not have adequate security controls to protect the confidentiality, integrity, and availability of its data and computer systems from threats originating outside its internal network.

Key Findings

- The Department of Education did not develop a comprehensive security management program nor did it allocate sufficient resources or personnel to adequately manage security. (Finding 1, page 5)

- The Department of Education had some firewall rules that were too permissive or unnecessary. (Finding 2, page 6)

- The Department of Education did not assess its monitoring needs nor did it proactively review security events. (Finding 4, page 8)

- The Department of Education had not adequately assessed, prioritized, reported, and remediated vulnerabilities. (Finding 5, page 9)

Audit Objective and Scope

The audit objective was to answer the following question:

- Did the Department of Education have adequate security controls to protect the department’s computer systems and data from threats originating outside the internal network?

We assessed controls as of February 2010.

Department of Education

Information Technology Security Controls

Overview

The Minnesota Department of Education is responsible for establishing education standards for grades prekindergarten through twelve and providing federal and state financial assistance to school districts to support the academic achievement of Minnesota's approximately 800,000 students.[1] The department annually administers approximately $7 billion in federal and state education funding. To perform its responsibilities, the department collects a significant amount of financial, student, staffing, and accountability data.

In February 2010, the department had about 45 information technology staff. Two of these staff were responsible for the day-to-day management of the department's network and servers, consisting of approximately 220 devices. Many of these devices support mission critical computer systems, while others, including the department's firewall, perform critical security functions.

Objective, Scope, and Methodology

The audit objective was to answer the following question:

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

To answer this question, we interviewed department staff and reviewed any 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 February 2010.

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

[1] Department of Education 2010-11 Biennial Budget Agency Profile.

management, patch management, anti-virus and anti-malware 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 Education did not have adequate security controls to protect the confidentiality, integrity, and availability of its data and computer systems from threats originating outside its internal network.

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

Findings and Recommendations

Finding 1

The Department of Education did not develop a comprehensive security management program nor did it allocate sufficient resources or personnel to adequately manage security.

The department did not develop a comprehensive security management program nor did it allocate sufficient resources or personnel to adequately manage security. Of most significance, the department had not designated a specific person, such as a chief information security officer, with the responsibility and authority to develop and enforce a security program. Instead, the department asserted that senior information technology management shared the responsibility for developing and managing a security program. However, these senior managers had not developed any formal security management plans, risk assessment methodologies, policies, standards, or procedures.

Without formal policies, standards, or procedures from the department's management, information technology staff had little guidance in performing their day-to-day tasks. Compounding the problem, the department was highly dependent on one employee, its network administrator, who was responsible for managing a high number of devices and critical processes, including the department's wired and wireless networks, servers, remote access technologies, firewall, vulnerability and threat management program, and security event monitoring. Daily operational tasks typically took priority over developing security practices.

A comprehensive security management program is a formal method used by an organization to effectively identify and manage risks throughout an organization and promptly respond to changing threats. Not unlike other important business functions, such as accounting and finance, the organization should establish the responsibility and authority for system security at its highest levels. The security program should be well managed and include proper planning and oversight activities.[2] Without a comprehensive security program, the department will likely be unable to effectively and proactively manage information technology risks and security. Findings 2 – 6 resulted from the department not having an effective security program.

[2] The National Institute of Standards and Technology developed special publications that provide guidance on planning, implementing, and managing an ongoing security management program.

Recommendation

- *The department should develop a comprehensive security management program for its information technology systems.*

  -- *It should define the program's scope, objectives, goals, and responsibilities and assess whether it has sufficient security staff to design, implement, and monitor the effectiveness of the security program.*

  -- *It should define and document the roles and responsibilities of individuals and groups that play a vital role in security and develop a training program to communicate their security responsibilities and to improve awareness of key risks and controls.*

  -- *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

The Department of Education had some firewall rules that were too permissive or unnecessary.

The department lacked formal firewall rule change procedures that included request, review, approval, and proper documentation, including the business purpose. The department also had not periodically reviewed and recertified the rules to ensure they were appropriate.

The department did not have a documented business purpose for about 75 percent of the approximately 800 firewall rules. Following a limited review of firewall rules with our auditors, the firewall administrator agreed that some rules were too permissive, outdated, unnecessary, in error, or in conflict with other rules. Also, the department had not used firewall rules or other mechanisms to prohibit the use of external connections to manage the firewall.

A poorly managed firewall increases the risk that the department's first line of defense against external hackers may not be adequate. 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.

Recommendations

- *The department should develop formal firewall management procedures, including change management procedures that include requesting, reviewing, approving, and documenting firewall rule changes. Procedures should also include the periodic review and recertification of the firewall rules.*

- *The department should conduct a complete review of its firewall rules. It should remove unneeded rules and further restrict excessively permissive rules.*

- *The department should prohibit external management of the firewall or other externally accessible computers.*

Finding 3

The Department of Education did not sufficiently restrict or filter computer traffic nor did it encrypt some sensitive computer traffic in its private internal network.

The department did not adequately restrict computer traffic in its private internal network. For example, it did not:

- Restrict or filter computer traffic from employee computers accessing internal computers from remote locations.

- Restrict or filter computer traffic between portions or segments of its private internal network.

- Limit the ability to log into critical devices, like the firewall, to specifically authorized internal computers belonging only to information technology staff.

The department did not encrypt some sensitive computer traffic in its private internal network. More specifically, it allowed information technology staff to use unencrypted connections when managing critical networking devices.

Network segmentation and filtering improve control by only allowing authorized traffic in or out of each segment on the private internal network. Without adequate segmentation and filtering, someone who gained unauthorized access to portions of the department's private internal network could attempt to move throughout the network and access any computer and software on them. Segmentation and filtering also help to prevent the spread of malicious software, such as viruses, worms, and trojans. Finally, unencrypted connections may allow an attacker to see sensitive information such as passwords.

Recommendations

- *The department should segment and filter computer traffic in its private internal network.*

- *The department should prohibit unencrypted connections from being used to manage the firewall and other devices.*

Finding 4

The Department of Education did not assess its monitoring needs nor did it proactively review security events.

The department's monitoring procedures were not sufficient 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's monitoring efforts were not effective, because it had not assessed which security-related events put its systems and data at highest risk. The department frequently logged all types of events, creating very large log files. However, the department did not regularly and proactively review any of its 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 have software to assist in the gathering and analyzing of security logs to identify events that require attention.

Finally, 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, the department would likely be unable to be proactive and take timely 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 acquiring technologies to facilitate the systematic review and analysis of security events.*

- *The department should define procedures for employees to follow when they identify a security incident.*

- *The department should define and follow its records retention requirements for security log records.*

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

Finding 5

The department routinely scanned its computers for vulnerabilities using the state's Enterprise Vulnerability Management System, however, it had not developed formal procedures to assess, prioritize, report, and remediate vulnerabilities.

The volume of data produced by the vulnerability management software can be very large. Without formal procedures, critical vulnerabilities may go unnoticed and not be resolved in a timely manner. 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 corrects critical vulnerabilities in a timely manner.*

The Department of Education had not periodically recertified remote access privileges nor did it implement strong password controls on some accounts.

Finding 6

The department had several weaknesses in the remote access it provided to some employees and its use of passwords to control and limit access to its network or network devices, as explained in the following bullets:

- The department did not periodically review and reconfirm the need for some employees to access the department's private internal network from outside the network. Over 20 employees with remote access had not used their accounts in over a year.

- 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 the network.

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

- The department had not changed some default passwords set by vendors for purchased technologies and software. Hackers can easily find default passwords on Internet websites and use them to gain unauthorized access.

Infrequently used user accounts provide an opportunity for exploitation by other employees or hackers because, if compromised, the misuse is less likely to be detected. Strong password controls are also important to help prevent employees and hackers from assuming the identity of legitimate system users and to enforce individual accountability.

Recommendations

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

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

- *The department should promptly change all default and easy to guess passwords.*

Minnesota Department of Education

May 3, 2010

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

Dear Mr. Nobles:

The Minnesota Office of the Legislative Auditor completed a security audit in February 2010 of the Minnesota Department of Education's security controls that help protect the department's computer systems and data from external threats. We agree the MDE lacks formally written policies and procedures for a comprehensive security management program for its information technology systems. After a MDE security management program is defined, an assessment of the staffing requirements to implement, and requirements to implement approved and funded formal security management written policies and procedures will be developed.

Without the formal policies and procedures MDE Information Technology team has taken external threats seriously as demonstrated by the early adoption of the Office of Enterprise Technology Enterprise Vulnerability Management System and the deployment of a web security appliance. We agree the overall effectiveness of these security technologies and other security devices will be enhanced with a formal security management program.

The Department's Information Technologies team has reviewed each finding and our response to the OLA audit findings and recommendations are:

1. **Finding - The Department of Education did not develop a comprehensive security management program nor did it allocate sufficient resources or personnel to adequately manage security.**

   Recommendation: The department should develop a comprehensive security management program for its information technology systems.

   a. MDE should define the program's scope, objectives, goals, and responsibilities and assess whether it has sufficient security staff to design, implement, and monitor the effectiveness of the security.

      MDE Response: We agree with the recommendation that the definition of the security management program will enhance the overall effectiveness of security within the Department. We will establish a Security Management Team to define, implement, and monitor the security management program. We have engaged with OET to leverage their Enterprise Security

Program Framework and thereby accelerate the establishment of the recommended security management program.

Person responsible: Cathy Wagner
Resolution Date: December 31, 2010

b. MDE should define and document the roles and responsibilities of individuals and groups that play a vital role in security and develop a training program to communicate their security responsibilities and to improve awareness of key risks and controls.

MDE Response: We agree with the recommendation.
Person responsible: John Paulson
Resolution Date: June 30, 2011

c. MDE should develop risk assessment methodologies and perform periodic assessments.

MDE Response: We agree with the recommendation.
Person responsible: Cathy Wagner
Resolution Date: June 30, 2012

d. MDE should develop written security policies, standards, and procedures and monitor compliance with them.

MDE Response: We agree with the recommendation.
Person responsible: John Paulson
Resolution Date: December 31, 2011

2. **Finding - The Department of Education did not have adequate procedures for managing its firewall.**

Recommendation:

a. The department should develop formal firewall management procedures, including change management procedures that include requesting, reviewing, approving, and documenting firewall rule changes. Procedures should also include the periodic review and recertification of the firewall rules.

MDE Response: We agree with the recommendation.
Person responsible: Mark Reker, IT Operations Manager
Resolution Date: June 30, 2011 dependent on MDE completion date for 1a and 1b.

b. The department should conduct a complete review of its firewall rules. It should remove unneeded rules and further restrict excessively permissive rules.

MDE Response: We agree with the recommendation. MDE Information Technologies has engaged with a vendor on the design, specifications and costs to replace existing firewall devices that are near vendor end of life. The plan is to submit for funding approval and complete this review with assistance from the vendor during the installation.

Person responsible: Mark Reker, IT Operations Manager
Resolution Date: December 31, 2010

c. The department should prohibit external management of the firewall or other externally accessible computers.

MDE Response: We agree with the recommendation.

Person responsible: Mark Reker, IT Operations Manager
Resolution Date: June 30, 2010

3. **Findings - The Department of Education did not sufficiently restrict or filter computer traffic in its private internal network nor did it encrypt some sensitive computer traffic.**

Recommendation:

a. The department should segment and filter computer traffic in its private internal network.

MDE Response: We agree with the recommendation. This recommendation will be addressed in the design of the firewall devices replacement discussed in MDE Response 2b.

Person responsible: Mark Reker, IT Operations Manager
Resolution Date: June 30, 2011

b. The department should prohibit unencrypted connections from being used to manage the firewall and other devices.

MDE Response: We agree with the recommendation. This recommendation will be addressed in the firewall devices replacement discussed in MDE Response 2b.

Person responsible: Mark Reker, IT Operations Manager
Resolution Date: December 31, 2010

4. **Findings - The Department of Education did not have effective monitoring procedures to detect and promptly respond to security-related events.**

Recommendation:

a. 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 acquiring technologies to facilitate the systematic review and analysis of security events.

MDE Response: We agree with the recommendation. This recommendation will be partially addressed in the firewall devices replacement discussed in MDE Response 2b. To fully address this will be dependent on the MDE completion date for 1a and 1b.

Person responsible: Mark Reker, IT Operations Manager
Resolution Date: June 30, 2011

b. The department should define procedures for employees to follow when they identify a security incident.

MDE Response: We agree with the recommendation. This will be dependent on the MDE completion date for 1a and 1b.

Person responsible: Mark Reker, IT Operations Manager
Resolution Date: June 30, 2011

c. The department should define and follow its records retention requirements for security log records.

MDE Response: We agree with the recommendation. This will be dependent on the MDE completion date for 1a and 1b.

Person responsible: Mark Reker, IT Operations Manager
Resolution Date: June 30, 2011

5. Findings - The Department of Education had not developed formal procedures to assess, prioritize, report, and remediate vulnerabilities.

Recommendation:

a. The department should develop a formal vulnerability and threat management program to ensure it corrects critical vulnerabilities in a timely manner

MDE Response: We agree with the recommendation. This will be dependent on the MDE completion date for 1a and 1b.

Person responsible: John Paulson
Resolution Date: June 30, 2011

6. The Department of Education had not implemented strong account and password controls.
While the department of education does require strong passwords for external users, we agree that we have not extended strong password requirements to our internal MDE users. Note: No non-MDE users have remote access.

Recommendation:

a. The department should periodically review and recertify those with remote access to ensure that they still require access.
MDE Response: We agree with the recommendation.

Person responsible: Mark Reker, IT Operations Manager

Resolution Date: December 31, 2011

b. The department should prohibit the sharing of passwords.
MDE Response: We agree with the recommendation. This recommendation will be partially addressed in the firewall devices replacement discussed in MDE Response 2b.

Person responsible: Mark Reker, IT Operations Manager
Resolution Date: December 31, 2011

c. The department should promptly change all default and easy to guess passwords.
MDE Response: We agree with the recommendation.

Person responsible: Mark Reker, IT Operations Manager
Resolution Date: June 30, 2010

Based on an analysis of the required work load to accomplish these recommendations on the timelines set forth in this letter we estimate the need for a base budget increase for the Information Technologies Division of approximately $500,000 for additional staff and software. As referenced in the security audit we are exceptionally understaffed on our network team and do not currently have a Chief Information Security Officer. To ensure that the documentation is completed and maintained on a timely basis we would need to add a project manager whose sole responsibilities would involve the inter-divisional coordination of risk management policies, procedures and documentation. In addition we would need two additional network engineers to accomplish the tactical activities needed to resolve these finding. The timelines outlined in this response can only be met with the addition of a minimum of four new positions. Without the additional staff these timelines cannot be met.

Sincerely,

Alice Seagren

Alice Seagren
Commissioner