OLA
OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA

FINANCIAL AUDIT DIVISION REPORT

Department of Labor and Industry

Information Technology Audit

As of November 2010

December 21, 2010 **Report 10-37**

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

OFFICE OF THE LEGISLATIVE AUDITOR
State of Minnesota • James Nobles, Legislative Auditor

December 21, 2010

Senator Ann H. Rest, Chair
Legislative Audit Commission

Members of the Legislative Audit Commission

Cindy Valentine, Acting Commissioner
Department of Labor and Industry

This report presents the results of our audit of the Department of Labor and Industry'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 department's staff on December 16, 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), Bill Betthauser (Senior Auditor), and Aimee Martin (Senior Auditor).

This report is intended for the information and use of the Legislative Audit Commission and the management of the Department of Labor and Industry. This restriction is not intended to limit the distribution of this report, which was released as a public document on December 21, 2010.

We received the full cooperation of the Department of Labor and Industry's staff while performing this audit.

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 Labor and Industry 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 Labor and Industry did not conduct formal risk assessments. (Finding 1, page 5)
- The Department of Labor and Industry's security plan template did not address some important security controls, and the department did not complete a security plan for all its critical technologies. (Finding 2, page 5)
- The Department of Labor and Industry did not update or patch the operating systems of some devices, leaving them susceptible to vulnerabilities. (Finding 3, page 6)
- The Department of Labor and Industry did not restrict computer traffic flow within its internal network nor did it restrict the ability to log in to critical computers to security administrators. (Finding 4, page 6)
- The Department of Labor and Industry did not implement formal change management processes to ensure that it adequately documented, assessed, tested, and approved proposed changes before implementing those changes in the technology environment. (Finding 5, page 7)

Audit Objective and Scope

The audit objective was to answer the following question:

- Did the Department of Labor and Industry 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 November 2010.

Department of Labor and Industry

Information Technology Security Controls

Overview

The Minnesota Department of Labor and Industry is responsible for enforcing state and federal workplace safety and labor standards and managing workers' compensation claims for injured workers. It is also responsible for adopting and administering building codes, conducting onsite inspections, and licensing construction-related professionals, such as electricians and plumbers. During fiscal year 2009, the department had approximately 480 employees and spent over $141 million, derived from various funding sources. Over half of the department's resources were appropriated from the Workers' Compensation Fund for the payment of workers' compensation claims and a special revenue fund financed by fees from the construction industry for permitting, licensing and inspections. The remainder of its resources came from the general, workforce development, and federal funds.[1]

The department's centralized information technology division employs about 25 individuals and is responsible for day-to-day management of the department's network and servers, consisting of approximately 560 devices.

Objective, Scope, and Methodology

The audit objective was to answer the following question:

- Did the Department of Labor and Industry 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 the department's staff 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 November 2010.

The audit focused on the department's controls that protected 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

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

computer network so that if one control fails, other controls will mitigate the risk of compromise. Examples of controls reviewed include network design, firewall 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 Labor and Industry 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.

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

Findings and Recommendations

Finding 1

The Department of Labor and Industry did not conduct formal risk assessments.

The department did not develop a strategy to periodically and formally assess risks relevant to its computer systems and data. The department had conducted some informal assessments and had categorized its systems based on the confidentiality, integrity, and availability requirements, but had not adopted and implemented a formal methodology to evaluate risks. Risk assessment methodologies provide a framework for consistently identifying, quantifying, and prioritizing risks related to its information assets. The results help management understand factors that can negatively influence operations and assist them in making informed decisions regarding the implementation of selected controls. The results also aid the department in developing and maintaining effective information security plans. If periodic risk assessments are not performed, risk to the organization could continue, unidentified and unmitigated, until the risk is realized.

Recommendation

- *The department should adopt a risk assessment methodology and perform periodic assessments.*

Finding 2

The Department of Labor and Industry's security plan template did not address some important security controls, and the department did not complete a security plan for all its critical technologies.

The department's security plan template did not consistently address certain critical security controls, such as documenting access roles, event logging, and remediation, password requirements, and change request and approval processes.[2] The quality of the security management program depends on the consideration of a wide range of controls to address risks that are inherent in the technology and the implementation of comprehensive security plans.

The department documented security plans for technologies that supported business applications, but did not document security plans for other key network infrastructures we examined. Security plans are the basis of the department's

[2] Office of Enterprise Technology's Technical Security Controls, Office of Enterprise Technology's Operational Security Controls, National Institute of Standards and Technology (NIST) Special Publication 800-18, and NIST Special Publication 800-53.

security program to ensure that technology staff implement consistent and appropriate practices across computing devices. Therefore, the overall effectiveness of the program relies on comprehensive and complete security plans documented on all devices.

Recommendations

- *The department should enhance security plan templates to address applicable controls from each NIST 800-53 security family.*
- *The department should complete security plans for all computer system network infrastructure and business technologies.*

Finding 3

The Department of Labor and Industry did not update or patch the operating systems of some devices, leaving them susceptible to vulnerabilities.

The manufacturers of all of the devices we reviewed had published notifications that they would no longer provide technical support for the devices' hardware, the operating system, or both. The department did not actively patch these devices; the department did not apply any updates or patches for some devices since their installation in 2005. Additionally, the department did not prioritize and scan these devices, as required by the state's vulnerability management standard.[3] Agencies that do not promptly fix critical vulnerabilities make their systems easy targets for computer hackers. The department did not determine the risk of the devices being compromised and did not implement plans to mitigate that risk.

Recommendation

- *The department should scan all devices and apply patches or other risk mitigation strategy within the timeframes specified by the vulnerability management standard.*

Finding 4

The Department of Labor and Industry did not restrict computer traffic flow within its internal network nor did it restrict the ability to log in to critical computers to security administrators.

The department did not adequately restrict computer traffic in its private internal network, as shown by the following examples:

- The department did not restrict computer traffic between portions or segments of its private internal network.

[3] Office of Enterprise Technology's Enterprise Vulnerability Management Security Standard 2010-02.

- The department did not sufficiently limit the ability to connect to critical devices, such as the firewall, to specifically authorized internal computers.
- The department did not exclusively use secure protocols for administering devices.

Network filtering improves controls by creating rules that only allow authorized traffic in or out of each segment on the private internal network. The risks of not having traffic restrictions is that a hacker, user, virus, or other malware that gained unauthorized access to a part of the department's internal network could attempt to move throughout the network and eavesdrop on data and voice traffic or attempt to access software and data on computers. If a portion of the network is compromised, implementing secure protocols with encryption limits the ability of an intruder to eavesdrop on the transmission of not public data on the network.

Recommendations

- *The department should implement network filters to restrict computer traffic between segments on its private internal network.*
- *The department should limit the ability to connect to critical devices to appropriate personnel.*
- *The department should implement and use only secure protocols for administering devices.*

Finding 5

The Department of Labor and Industry did not implement formal change management processes to ensure that it adequately documented, assessed, tested, and approved proposed changes before implementing those changes in the technology environment.

The department had an informal process to assess changes to the technology environment. While many of the changes were discussed in regular security meetings, the department did not have guidelines for how it would track, assess, test, authorize, or document changes.

If system change requests are not assessed in a consistent manner, changes could be made that weaken the network's security or affect the availability of critical technology.

Recommendation

- *The department should implement a change management process that establishes the roles and responsibilities for assessing, testing, approving, and documenting changes to the technology environment.*

443 Lafayette Road N.
St. Paul, Minnesota 55155
www.dli.mn.gov

MINNESOTA DEPARTMENT OF
LABOR & INDUSTRY

(651) 284-5005
1-800-DIAL-DLI
TTY: (651) 297-4198

December 16, 2010

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

Dear Mr. Nobles,

I would like to thank the Office of the Legislative Auditor and your team for the work on this information security controls audit at the Minnesota Department of Labor and Industry (DLI). We appreciate the review and assessment provided by your team through this audit. We agree with all of the findings put forth in the audit and appreciate the recommendations for improvement.

DLI values the audit's conclusion that "DLI generally has adequate security controls already in place", and we will continue moving our efforts forward based upon the recommendations outlined in the final report.

Below you will find our specific responses to the findings and recommendations:

1. **Finding - The Department of Labor and Industry did not conduct formal risk assessments.**

   Recommendation:

   The department should adopt a risk assessment methodology and perform periodic assessments.

   Response: The department agrees with the finding and recommendation. DLI will begin to formalize its risk assessment program and process by examining and evaluating risk assessment strategies and methodologies.

   Responsibility: DLI Chief Information Officer (CIO) and Network Security Group (NSG)

   Resolution Date: 12/31/2011

2. **Finding - The Department of Labor and Industry's security plan template did not address some important security controls, and the department did not complete a security plan for all its critical technologies.**

Recommendations:

The department should enhance security plan templates to address applicable controls from each NIST 800-53 security family.

Response: The department agrees with the finding and recommendation. DLI will modify templates to be compliant with NIST 800-53.

Responsibility: NSG

Resolution Date: 6/30/11

The department should complete security plans for all computer system network infrastructure and business technologies.

Response: The department agrees with the finding and recommendation. DLI will create security plans for devices that currently have none.

Responsibility: NSG

Resolution Date: 6/30/11

3. **Finding - The Department of Labor and Industry did not update or patch the operating systems of some devices, leaving them susceptible to vulnerabilities.**

Recommendation:

The department should scan all devices and apply patches or other risk mitigation strategy within the timeframes specified by the Vulnerability Management Standard.

Response: The department agrees with the finding and recommendation. DLI will begin scanning devices that were previously not included. We will develop a plan to replace devices that are nearing vendor end of life. In the interim, we will patch system vulnerabilities uncovered in the scan.

Responsibility: NSG

Resolution Date: 1/31/2011

4. **Finding - The Department of Labor and Industry did not restrict computer traffic flow within its internal network nor did it restrict the ability to log in to critical computers to security administrators.**

Recommendations:

The department should implement network filters to restrict computer traffic between segments on its private internal network.

Response: The department agrees with the finding and recommendation. DLI will develop a plan to address this finding.

Responsibility: Network Administrator

Resolution Date: 1/31/2011

The department should limit the ability to connect to critical devices to appropriate personnel.

Response: The department agrees with the finding and recommendation. DLI will limit access to critical devices to administrators only.

Responsibility: NSG

Resolution Date: 1/31/2011

The department should implement and use only secure protocols for administering devices.

Response: The department agrees with the finding and recommendation. DLI will restrict administrative access to devices to the use of secure protocols.

Responsibility: Network Administrator

Resolution Date: 1/31/2011

5. Finding - The Department of Labor and Industry did not implement formal change management processes to ensure that it adequately documented, assessed, tested, and approved proposed changes before implementing those changes in the technology environment.

Recommendation:

The department should implement a change management process that establishes the roles and responsibilities for assessing, testing, approving, and documenting changes to the technology environment.

Response: The department agrees with the finding and recommendation. DLI will develop and implement formal procedures.

Responsibility: NSG

Resolution Date: 12/31/2010

Sincerely,

Cynthia Valentine

Cynthia Valentine
Acting Commissioner
Minnesota Department of Labor and Industry