OLA

OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA

Information Technology Audit

Department of Revenue

Selected Individual Income Tax Processing Controls

MARCH 18, 2004 **04-16**

Financial Audit Division

The Office of the Legislative Auditor (OLA) is a professional, nonpartisan office in the legislative branch of Minnesota state government. Its principal responsibility is to audit and evaluate the agencies and programs of state government (the State Auditor audits local governments).

OLA's 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 also investigates allegations that state resources have been used inappropriately.

The division has a staff of approximately 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.

Consistent with OLA's mission, the Financial Audit Division works to:

- Promote Accountability,
- Strengthen Legislative Oversight, and
- Support Good Financial Management.

Through its Program Evaluation Division, OLA conducts several evaluations each year.

OLA is under the direction of the Legislative Auditor, who is appointed for a six-year term by the Legislative Audit Commission (LAC). The LAC is a bipartisan commission of representatives and senators. It annually selects topics for the Program Evaluation Division, but is generally not involved in scheduling financial audits.

All findings, conclusions, and recommendations in reports issued by the Office of the Legislative Auditor are solely the responsibility of the office and may not reflect the views of the LAC, its individual members, or other members of the Minnesota Legislature.

This document can be made available in alternative formats, such as large print, Braille, or audio tape, by calling 651-296-1235 (voice), or the Minnesota Relay Service at 651-297-5353 or 1-800-627-3529.

All OLA reports are available at our Web Site: http://www.auditor.leg.state.mn.us

If you have comments about our work, or you want to suggest an audit, investigation, or evaluation, please contact us at 651-296-4708 or by e-mail at auditor@state.mn.us

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

Representative Tim Wilkin, Chair
Legislative Audit Commission

Members of the Legislative Audit Commission

Mr. Dan Salomone, Commissioner
Minnesota Department of Revenue

We have conducted an information technology audit of selected components of the systems that support individual income tax processing. The primary purpose of this audit was to determine if the Department of Revenue had controls to protect the integrity and confidentiality of individual income tax data. However, we also examined selected controls over the depositing and recording of individual income tax revenues. Our audit scope included a review of internal controls as of November 2003.

We conducted our audit in accordance with auditing standards generally accepted in the United States of America contained in *Government Auditing Standards*, issued by the Comptroller General of the United States. Those standards require that we obtain an understanding of management controls relevant to the audit. The standards also require that we design the audit to provide reasonable assurance that the Department of Revenue complied with provisions of laws, regulations, contracts, and grants that are significant to the audit. The department's management is responsible for establishing and maintaining the internal control structure and complying with applicable laws, regulations, contracts, and grants.

Information technology audits frequently include the review of sensitive security data that is legally classified as nonpublic under the Minnesota Data Practices Act. In some cases, to protect state resources and comply with the Minnesota Data Practices Act, we must withhold security-related details from our publicly released report. When these situations occur, we communicate all pertinent details to agency leaders in a separate, confidential document. For this audit, we issued five separate, confidential documents to the management of the Department of Revenue.

This report is intended for the information of the Legislative Audit Commission and the management of the Department of Revenue. This restriction is not intended to limit the distribution of this report, which was released as a public document on March 18, 2004.

/s/ James R. Nobles

James R. Nobles
Legislative Auditor

/s/ Claudia J. Gudvangen

Claudia J. Gudvangen, CPA
Deputy Legislative Auditor

End of Fieldwork: November 30, 2003

Report Signed On: March 15, 2004

Room 140, 658 Cedar Street, St. Paul, Minnesota 55155-1603 • Tel: 651/296-4708 • Fax: 651/296-4712
E-mail: auditor@state.mn.us • TDD Relay: 651/297-5353 • Website: www.auditor.leg.state.mn.us

Table of Contents

Audit Participation

The following members of the Office of the Legislative Auditor prepared this report:

Claudia Gudvangen, CPA	Deputy Legislative Auditor
Christopher Buse, CPA, CISA, CISSP	Information Technology Audit Manager
Eric Wion, CPA, CISA	Auditor-in-Charge
Neal Dawson, CPA, CISA	Information Technology Auditor
Carl Otto, CPA, CISA	Information Technology Auditor

Exit Conference

We discussed the results of the audit with the following staff of the Department of Revenue at an exit conference on March 8, 2004:

Dan Salomone	Commissioner
Dennis Erno	Deputy Commissioner
Stephen Stedman	Chief Information Officer
Bruce Showel	Chief Information Security Officer
Jerry Hanson	Information Systems Director
Dan Ostdiek	Financial Management Director
Steve Krovitz	Internal Auditor

Minnesota Department of Revenue
Selected Individual Income Tax Processing Controls

Report Summary

Overall Audit Conclusions

The Minnesota Department of Revenue developed multiple layers of security to protect the integrity and confidentiality of individual income tax data. However, we found shortcomings in this security infrastructure that exposed tax data to an unnecessary risk of loss or misuse. The department needs to remedy the specific security weaknesses that we brought to its attention and strengthen its policies, procedures, and standards to reduce the possibility of additional weaknesses surfacing in the future.

Key Findings

- The department's overall security program lacks important ingredients. Specifically, the department has not conducted formal information technology risk assessments or documented baseline security procedures and standards for its income tax processing systems. The department also has not validated the effectiveness of or adequately monitored its security controls. (Finding 1, page 7)
- The department had weaknesses in its controls over authenticating the identity of system users and managing their security clearances. (Findings 2 through 5, pages 8 - 11)
- The department had too many points of access into its private network. (Finding 6, page 11)
- The department had weaknesses in its server configuration and maintenance procedures. (Findings 7 and 8, pages 12 - 13)
- The department also has not established sufficient monitoring controls to identify and promptly respond to potential security breaches. (Finding 9, page 13)

Background

This information technology audit assessed the adequacy of selected individual income tax processing controls. We designed our work to determine if the department had adequate controls to protect the integrity and confidentiality of individual income tax data. We also assessed the adequacy of controls over the depositing and recording of individual income tax revenues. Individual income taxes are the largest revenue source for the State of Minnesota. During fiscal year 2003, the $5.5 billion of individual income tax accounted for approximately 43 percent of all revenue in the State of Minnesota's General Fund.

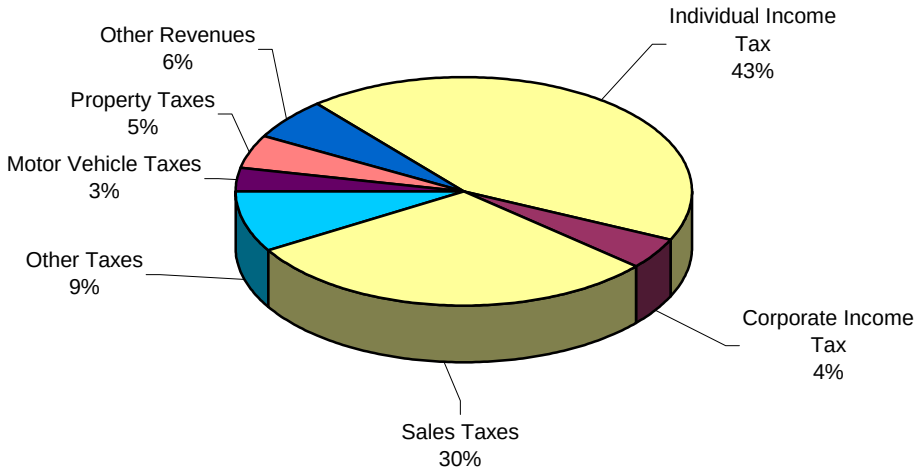
This page intentionally left blank.

Chapter 1. Introduction

This information technology audit assessed the adequacy of selected individual income tax processing "general" and "application" controls. General controls are those controls that apply to all business systems that run in a specific computerized environment. Computer security policies, procedures, and standards are examples of general controls. Application controls, on the other hand, are unique to specific computerized business systems. Application controls filter out invalid data before it can be processed and ensure that remaining transactions are completely and accurately processed. Application controls include both manual procedures, such as reconciliations, as well as computerized edit programs. Together, general and application controls help protect the integrity and confidentiality of critical business data.

The Minnesota Department of Revenue collects 28 different taxes. Annually, these taxes provide most of the money that funds Minnesota state government. As illustrated in Figure 1-1, the Individual Income Tax is the largest revenue source for the State of Minnesota. During fiscal year 2003, the $5.5 billion of individual income tax accounted for approximately 43 percent of all revenues in the State of Minnesota's General Fund.

Figure 1-1
General Fund Revenue Sources
Fiscal Year 2003



Source: State of Minnesota's 2003 Comprehensive Annual Financial Report.

Minnesota Department of Revenue
Selected Individual Income Tax Processing Controls

The vast majority of all individual income tax revenues comes from businesses that withhold payroll taxes from their employees. Approximately 160,000 businesses remit withholdings to the department. The department also collects some individual income tax revenue directly from taxpayers when they pay estimated tax or file their returns. Approximately 2.4 million people file individual income tax returns.

The department developed many integrated computer systems to handle the various aspects of individual income tax processing. Most of these systems run on powerful computers that are commonly referred to as file servers. However, some individual income tax processing occurs on large mainframe computers. The department utilizes a variety of different operating systems on these computers and stores data in several different database management systems. Information technology professionals in the department designed most of the computer programs that process individual income tax revenues and data. However, the department also purchased some tax processing software from vendors.

The department developed many layers of security to protect the integrity and confidentiality of individual income tax data. For example, the department installed firewalls and other perimeter security devices to keep hackers out of its private network. Inside its network, the department deployed many security tools to limit employees to the minimum clearances necessary to fulfill their job duties. Most of these security tools are integrated components of computer operating and database management systems. However, the department also developed some of its own software to meet its unique security needs.

The primary objective of this audit was to assess the adequacy of individual income tax security controls. However, we also examined selected controls over depositing and recording individual income tax revenues. Chapter 2 discusses our scope, objectives, and methodology in more detail.

We obtained our evaluation criteria from several sources, including the Control Objectives for Information and Related Technologies (COBIT). Published by the Information Systems Audit and Control Foundation, the COBIT framework consists of 34 high-level control objectives and 318 detailed control objectives. COBIT groups these objectives into four domains: Planning and Organization, Acquisition and Implementation, Delivery and Support, and Monitoring. We obtained additional evaluation criteria from publications provided by hardware and software manufacturers whose products are used in individual income tax processing.

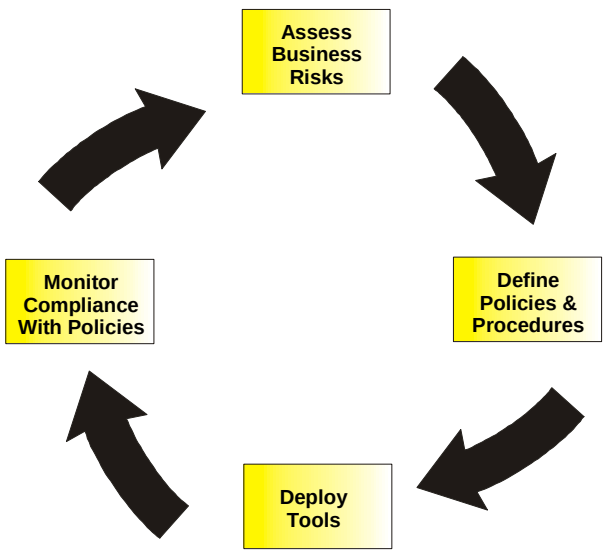
Chapter 2. Selected Individual Income Tax General and Application Controls

Chapter Conclusions

The Minnesota Department of Revenue developed multiple layers of security to protect the integrity and confidentiality of individual income tax data. However, we found shortcomings in this security infrastructure that exposed tax data to an unnecessary risk of loss or misuse. Of greatest concern, the department has not conducted formal information technology risk assessments or documented baseline security standards for its income tax processing systems. The department also has not established sufficient monitoring controls to identify and promptly respond to potential security breaches. These shortcomings contributed to a wide array of security weaknesses. The department needs to remedy the specific security weaknesses that we brought to its attention and strengthen its policies, procedures, and standards to reduce the possibility of additional weaknesses surfacing in the future.

Every organization needs strong security controls to protect its critical business data. However, even with strong controls, it is impossible to be completely secure. This fact makes designing and implementing a security infrastructure an ongoing exercise in risk management. As illustrated in Figure 2-1, organizations typically begin this process by performing a detailed risk analysis to identify potential vulnerabilities. The results of this analysis help organizations design policies and procedures to reduce their exposures to a level that executive management is willing to accept. Security professionals then deploy tools, such as access control software, to enforce the policies and procedures that management sanctioned. Information provided by these tools helps organizations monitor compliance with their policies and procedures and fine-

Figure 2-1
The Ongoing Security Management Lifecycle



Source: Auditor prepared.

tune subsequent risk assessments in the ongoing security management lifecycle. These fundamental activities allow an organization to proactively manage information security risks, rather than react to problems after they have occurred.

Audit Objective and Methodology

This information technology audit assessed the adequacy of selected individual income tax processing general and application controls. Our work focused on key technologies used by the department to collect, record, and secure individual income tax revenues and data. Specifically, we designed our work to answer the following questions:

- Did the department design and implement adequate controls to protect the integrity and confidentiality of individual income tax data?

- Did the department design and implement adequate controls over the depositing and recording of individual income tax revenues?

To answer these questions, we interviewed employees to gain an understanding of how individual income tax data and money flows through various systems and divisions within the department. We gathered and reviewed documentation for significant security and financial controls performed by employees and embedded in computerized processes. We also used computer-assisted audit and vulnerability assessment tools to test critical controls in computer operating systems, database management systems, and perimeter security devices. Finally, we examined custom security features that the department developed for its tax processing systems.

Conclusions

The department's security program was not built on a foundation of policies, procedures, and standards. Furthermore, it lacks important monitoring controls to detect and promptly respond to security events. We feel that these overall security program shortcomings, discussed in Finding 1, contributed to the other findings described in this report. Findings 2 through 5 discuss weaknesses in procedures used to confirm the identity of system users and manage their security clearances. Findings 6 through 8 discuss server configuration and maintenance issues that came to our attention. And finally, Finding 9 outlines weaknesses in the monitoring controls deployed by the department.

This public report discusses the results of our audit at a very high level. However, by design it does not elaborate on specific security weaknesses that came to our attention. We communicated pertinent details of all security weaknesses to the department during the course of our audit. We also provided the department with five confidential documents that included the details underlying each finding in this report.

Current Findings and Recommendations

1. The department's overall security program lacks important ingredients.

The department deployed many security tools to protect individual income tax data. However, shortcomings in other aspects of its security program diminished the effectiveness of these tools. Of greatest concern, the department has not conducted formal information technology risk assessments or documented baseline security procedures and standards for its income tax processing systems. The department also has not established sufficient monitoring controls to identify and promptly respond to potential security breaches. These security program shortcomings contributed to a wide array of security weaknesses that we brought to management's attention. Left unaddressed, these shortcomings will undoubtedly lead to a further degradation of security controls.

Management did not define or document important security infrastructure planning decisions. Without this documentation, we were unable to find clear answers to many fundamental security questions, such as:

- What types of security clearances are appropriate for different types of employees?
- Who is responsible for approving access requests for each income tax processing system?
- Who is responsible for configuring security tools and entering security transactions for each system?
- What types of security events should be logged, investigated, and brought to management's attention?

As illustrated in Figure 2-1, these and other important security decisions are the product of an ongoing risk management process. Most risk management methodologies include steps to identify potential vulnerabilities, estimate the likelihood of their exploit, and assess the potential impact. The resulting risk assessment data helps organizations design security policies, procedures, and detailed standards that are commensurate with risk.

Though management communicated its commitment to security in broad policies, it did not transform these policies into detailed security standards for specific systems. Documenting this information is vital because it provides security professionals with criteria to configure security tools and make consistent security decisions. Documentation also helps ensure the continued understanding and operation of critical security controls, should key employees leave the organization.

Finally, the department did not validate the effectiveness of or adequately monitor its security controls. We found no evidence to indicate that independent persons had ever assessed the adequacy of security controls for most systems that we examined. The department also did not run vulnerability assessment tools to search for commonly known and exploitable weaknesses. Vulnerability scanners are special software packages that probe systems to find security weaknesses. Though security events for some systems were logged, the department rarely reviewed these logs for signs of attack or inappropriate system usage by employees.

Recommendations

- *The department should perform periodic information technology risk assessments and use that information to develop detailed security baselines for its systems.*

- *The department should periodically validate the adequacy of its controls through independent assessments.*

2. Access request procedures are weak in several respects.

Procedures for requesting and granting access to systems have not been clearly defined, documented, or communicated to decision makers. Explicit procedures help foster security decisions that are consistent, logical, and in compliance with management's intentions. Explicit procedures are particularly important in complex environments with highly sensitive data, such as individual income tax processing.

Haphazard practices have evolved in the absence of clearly defined procedures. Supervisors currently contact multiple security liaisons to request access to tax processing systems, using a variety of methods. Several methods that we observed, such as Email messages and phone conversations, are susceptible to fabrication. Many security transactions that we tested had no underlying documentation, such as an access request form. When questioned, the department told us that these security transactions might have been initiated from phone calls or Email messages that were not retained. We found little documentation to help supervisors understand the types of standard security clearances that were created for specific groups of employees. Without this documentation, we question whether supervisors had sufficient information to make informed security decisions. We also question whether security liaisons had sufficient information to challenge the propriety of access requests. Finally, some transactions appear to have been entered by information technology professionals, rather than the security liaisons designated by the department to approve access requests.

Controls over granting access to information technology professionals were particularly weak. Information technology professionals had the most powerful accounts on each system that we reviewed. However, the department had virtually no documentation describing what clearances these employees needed to fulfill their job duties. The department also did not define who was responsible for reviewing, authorizing, and creating accounts for these employees. Finding 5 discusses information technology professionals with excessive security clearances in more detail.

Recommendation

- *The department should define, document, and communicate access request procedures that include:*

- *types of security clearances that are appropriate for all types of employees, including information technology professionals;*
- *acceptable methods to communicate access requests;*
- *retention requirements for access request documentation; and*
- *persons responsible for approving requests and entering security transactions.*

3. Procedures for modifying and revoking security clearances are not effective.

The department does not have effective procedures to identify and modify security clearances for people whose job duties changed or who have resigned. Currently, supervisors are responsible for notifying the appropriate security liaisons when members of their staff have employment condition changes. However, we found many employees whose security clearances had not been modified or revoked even though they had changed jobs or no longer worked for the department. We also found many accounts that had not been used in over 120 days, which suggested that they may no longer be needed.

Internal controls that place complete reliance on human interaction are prone to error. Therefore, we encourage the department to search for automated processes to supplement or replace its supervisor notifications. One solution may be to have human resources personnel communicate all employment condition changes directly to dedicated security liaisons. Requiring periodic recertification of all security clearances is another effective way to identify people with system access that is no longer needed.

Recommendation

- *The department should adopt additional controls to identify and modify security clearances for people whose employment conditions change.*

4. Controls used to confirm the identity of system users were weak in several respects.

The department did not deploy sufficient controls to secure accounts that have access to individual income tax processing systems. These controls make it more difficult for unscrupulous individuals to hijack the identity of legitimate system users. The department also allowed some employees to share accounts, thereby diminishing the ability to trace certain actions to specific people. 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 vigorously enforce these principles exposes the tax processing systems and their data to unnecessary risks.

We question the appropriateness of the method used by the department to authenticate the identity of information technology professionals and other employees with extremely powerful security clearances. The department relies on unique accounts and passwords to authenticate the

identity of people who attempt to access its individual income tax processing systems. This authentication approach is called "single factor" authentication because it places complete reliance on a secret password that should only be known by one person. Organizations that deploy highly sensitive computer systems often supplement secret passwords with additional authentication controls, such as smart cards or biometric devices. The key issue in deciding whether to move from single to multifactor authentication is the risk of having a password compromised. Individual income tax is the largest source of revenue for the State of Minnesota. Furthermore, individual income tax data is extremely sensitive and merits the utmost protection to prevent unauthorized disclosure. Recognizing these facts, we challenge the department to search for more robust ways to authenticate the identity of people with access to its systems.

The department did not configure some computers 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 operating and database management systems have features that can be customized to enforce strong password controls. For example, features can be enabled that prevent users from selecting blank passwords or words that are in the dictionary. We examined these and other customizable security features and found many weaknesses. In some cases, the department did not implement important security controls. In others, security features were implemented, but some accounts were permitted to circumvent those controls.

The department did not change the default passwords on some purchased software products. Many purchased software products come with default user accounts and passwords. It is important to immediately change default passwords because they provide an easy avenue for hackers to gain unauthorized access. In fact, lists of default accounts and passwords for most purchased software products can be downloaded from the Internet. During our audit, we were able to take control of some software because the department failed to change the default passwords.

Finally, some information technology professionals share accounts with extremely powerful security clearances. Sharing passwords is always unacceptable because it destroys individual accountability. Once a password has been shared, it is virtually impossible to prove that a specific person initiated a specific computerized transaction.

Recommendations

- *The department should explore more robust ways to authenticate the identity of people with access to individual income tax processing systems.*
- *The department should implement and enforce comprehensive password management controls.*
- *The department should implement controls to ensure that critical system activities can be traced to specific individuals.*
- *The department should immediately change the default passwords after installing software.*

5. Many people had excessive clearance to individual income tax systems and data.

During our audit, we identified many people with security clearances that exceeded what was necessary to fulfill their job duties. We also found some accounts used by software products that had been assigned unnecessary clearances. As discussed in Finding 1, the department has not defined the types of security clearances that are appropriate for different types of employees. Without such documentation, we could not determine if management had sanctioned these or other powerful security clearances.

Most accounts with excessive security clearances belonged to information technology professionals. For example, some people had clearance to enter security transactions even though they were not responsible for performing security duties. We also identified 13 system developers that had clearance to enter any individual income tax transaction. System developers typically work in a test environment and do not need access to production systems or data. Many people had unnecessary access to the programs and data underlying the tax return imaging system. And finally, through an improperly secured database, over 50 people had clearance to read sensitive individual income tax data. When questioned, the department could not explain why many of these employees needed such access. Granting direct access to databases is risky because it could allow people to circumvent confidential data monitoring controls.

Recommendation

- *The department should examine all employees' security clearances to ensure that they are commensurate with their job duties.*

6. The department had too many points of access into its private network.

The department installed modems and software on many of its computers to allow people to connect to and operate their computers from remote locations, such as their homes. Many of these network access points were not under the direct control of information technology professionals who were responsible for perimeter security.

Providing numerous network access points makes it extremely difficult to manage security. With multiple access points, information technology professionals must configure and maintain remote connectivity software on many machines. They also must monitor many different computers for signs of a remote attack. Finally, configuration errors on any one of these machines could expose the entire private network to security breaches.

Recommendations

- *The department should limit access points into its private network to the minimum number necessary to conduct business.*

- *All network access points should be managed, secured, and monitored by information technology professionals.*

7. Some computers were running unnecessary and insecure services.

We identified many services on individual income tax servers that were not necessary. The term "service" refers to a computer program that runs continuously, listening for specific commands. Services are typically activated by default after installing a computer operating system and are needed to perform basic functions, such as logging in. However, many services are not necessary and could lead to security breaches if not removed.

In several cases, unnecessary services that were running on computers that we tested were susceptible to common hacker exploits. We also found other insecure services that were used by the department to conduct business. However, secure replacements were available but not deployed.

Recommendations

- *The department should remove all unnecessary services from individual income tax processing computers.*

- *The department should replace all remaining services that have known security weaknesses with more secure programs.*

8. The department did not promptly perform important system maintenance procedures.

We identified some security-related software patches that were not installed on the computers that support individual income tax processing. The department uses many commercially available software packages. Unfortunately, computer hackers routinely discover and exploit flaws in commercial software to gain unauthorized access to organizations' computer systems. When these exploits occur, reputable vendors immediately develop and publish software patches to correct the deficiencies in their products. Organizations that do not promptly install these software patches make their systems easy targets for computer hackers.

Identifying and patching computers can be an extremely daunting task, particularly in environments like the Department of Revenue that have hundreds of computers. To improve controls, the department needs to define and document patch management policies and procedures. The department also should search for automated solutions to streamline patch management tasks. Currently, information technology professionals install patches manually on most servers.

Recommendation

- *The department should implement procedures to promptly install security-related patches.*

9. The department does not adequately monitor its systems.

The department lacked important controls to detect and promptly respond to security-related events, such as unauthorized access attempts. The best security controls are those that prevent inappropriate events from happening. Unfortunately, though, it is virtually impossible to design flawless preventive defenses. It is a sad reality that unscrupulous individuals discover new security exploits daily and use that knowledge to penetrate organizations with many layers of preventive defenses. This inherent security administration problem is why every organization must vigilantly monitor its systems for signs of attack. Since time is of the essence when under attack, every organization also must have decisive incident response procedures. Organizations that do not have effective procedures may fail to discover that they are completely unsecured until extensive damage has been done.

The department did not adequately assess its monitoring needs or actively monitor security-related events. Some commercial software products used by the department can be customized to log certain types of unusual events and alert specific individuals. However, in some cases these products were not configured to log any events. In others, employees did not routinely review the activities that were logged. When questioned, employees told us that they did not have sufficient resources to review logs on a regular basis.

Recommendation

- *The department should assess it monitoring needs and develop procedures to monitor its systems on an ongoing basis.*

This page intentionally left blank.

March 12, 2004

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

Dear Mr. Nobles:

This is in reply to a series of recommendations made by the Office of Legislative Auditor (OLA) in connection with its audit of the security policies and practices associated with the Department of Revenue's income tax return processing systems. The audit examined nine major aspects of security and included one or more recommendations for each element of security studied.

The department agrees with all recommendations made by the OLA. Here is the department's response to those recommendations.

1. Overall Security Program

Recommendation: The department should perform periodic information technology risk assessments and use that information to develop detailed security baselines for its systems.

Response: Assessments of the information technology risks of the department's applications, hardware and systems are currently in progress and will result in detailed baselines for minimum security.

Person Responsible: Bruce Showel, Information Security
Implementation Date: June 30, 2005

Recommendation: The department should periodically validate the adequacy of its controls through independent assessments.

Response: The department understands the need for independent assessments of its controls and intends to carry out a controls assessment in the near future. Due to limited financial resources the department cannot immediately commence such independent assessments.

Person Responsible: Bruce Showel, Information Security
Implementation Date: Unknown at this time

2. Access Request Procedures

Recommendation: The department should define, document and communicate access request procedures that include:

Commissioner's Office
Mail Station 7100
St. Paul, MN 55146-7100

Tel: 651-296-3403
Fax: 651-556-3100
Minnesota Relay (TTY) 711
An equal opportunity employer

- Type of security clearances that are appropriate for all types of employees including information technology professionals;
- Acceptable methods to communicate access requests;
- Retention requirements for access request documentation; and
- Persons responsible for approving requests and entering security transactions.

Response: Internal authentication processes related to the definition, documentation and communication of access request procedures have regularly been identified as an area of concern and proposals have been developed to address it as soon as the availability of financial resources permit.

Person Responsible: Bruce Showel, Information Security
Implementation Date: Unknown at this time

3. Procedures for Modifying and Revoking Security Clearances

Recommendation: The department should adopt additional controls to identify and modify security clearances for people whose employment conditions change.

Response: Internal authentication processes related to the identification and modification of security clearances have regularly been identified as an area of concern. Proposals to address this concern have been developed and will be implemented as soon as the availability of financial resources permit.

Person Responsible: Bruce Showel, Information Security
Implementation Date: Unknown at this time

4. Controls Used to Confirm the Identity of System Users

Recommendation: The department should explore more robust ways to authenticate the identity of people with access to individual income tax processing systems.

Response: Processes related to authenticating the identity of individuals have regularly been identified as an area of concern. Proposals that address this concern have been developed and will be implemented as soon as financial resources permit.

Person Responsible: Bruce Showel, Information Security
Implementation Date: Unknown at this time

Recommendation: The department should implement and enforce comprehensive password management controls.

Response: The department has implemented and enforces comprehensive password management controls. The instances where this was not the case will be addressed.

Person Responsible: Bruce Showel, Information Security
Implementation Date: June 30, 2004

Recommendation: The department should implement controls to ensure that critical system activities can be traced to specific individuals.

Response: The department has implemented controls to ensure that access to individual tax systems can be traced to specific individuals for all front line users. Appropriate

controls will be added to ensure that information technology (IT) professionals are held to the same level of accountability.

Person Responsible: Bruce Showel, Information Security
Implementation Date: Unknown at this time

Recommendation: The department should immediately change the default passwords after installing software.

Response: The department has made these changes. Procedures will also be updated to minimize the risk of acquiring and implementing software without changing the default passwords.

Person Responsible: Jerry Hanson, Information Systems Division
Implementation Date: Completed

5. Clearance to Individual Income Tax Systems and Data

Recommendation: The department should examine all employees' security clearances to ensure that they are commensurate with their job duties.

Response: A review of the appropriate employee security clearances will be verified with supervisors to check whether each employee has the appropriate level of access.

Person Responsible: Bruce Showel, Information Security
Implementation Date: Unknown at this time

6. Points of Access into Private Network

Recommendation: The department should limit access points into its private network to the minimum number necessary to conduct business.

Response: The number of access points into the department's private network have continually been reduced. The department will be developing a detailed policy to further limit access points.

Person Responsible: Jerry Hanson, Information Systems Division
Implementation Date: Unknown at this time

Recommendation: All network access points should be managed, secured and monitored by information technology professionals.

Response: The department is identifying methods and tools with which to manage, secure and monitor its network access points, pending the availability of financial resources. The department's remote access policy will be modified to address IT and occasional users who access the network.

Persons Responsible: Jerry Hanson and Bruce Showel
Implementation Date: Unknown at this time

7. Running Unnecessary and Insecure Services

Recommendation: The department should remove all unnecessary services from individual income tax processing computers.

Response: Procedures will be updated to ensure that all unnecessary services are removed.

Person Responsible: Jerry Hanson, Information Systems Division
Implementation Date: June 30, 2004

Recommendation: The department should replace all remaining services that have known security weaknesses with more secure programs.

Response: Procedures will be updated to ensure that all services with known security weaknesses are replaced with more secure programs and the replacements can be performed without hampering department activities.

Person Responsible: Jerry Hanson, Information Systems Division
Implementation Date: Unknown at this time

8. System Maintenance Procedures

Recommendation: The department should implement procedures to promptly install security related patches.

Response: Procedures will be updated to ensure that all security patches are installed, and that the patches are adequately tested to make sure they do not disrupt the current functionality of the systems. The department will also investigate automated solutions for streamlining the patch management tasks, subject to the availability of resources.

Person Responsible: Jerry Hanson, Information Systems Division
Implementation Date: Unknown at this time

9. Monitoring Systems

Recommendation: The department should assess it monitoring needs and develop procedures to monitor its systems on an ongoing basis.

Response: System monitoring procedures and processes will be updated and implemented, subject to the availability of financial resources.

Persons Responsible: Jerry Hanson and Bruce Showel
Implementation Date: Unknown at this time

On behalf of the department, we would like to thank you and your staff for the helpful recommendations and assistance provided to our agency.

Sincerely,

/s/ Steve Stedman

Steve Stedman
Chief Information Officer

/s/ Dennis Erno

Dennis Erno
Deputy Commissioner