OLA
OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA

FINANCIAL AUDIT DIVISION REPORT

Small Agencies' Information Security Controls

Information Technology Audit

April 9, 2009 **Report 09-16**

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

April 9, 2009

Senator Ann H. Rest, Chair
Legislative Audit Commission

Members of the Legislative Audit Commission

Mr. Gopal Khanna, State Chief Information Officer
Office of Enterprise Technology

Mr. Christopher Buse, Chief Information Security Officer
Office of Enterprise Technology

This report presents the results of our information technology audit of small agencies' security controls. The scope of our audit focused on controls that help to protect the integrity, confidentiality, and availability of the agencies' computer systems and data. 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 each individual agency in January 2009. We also met with Office of Enterprise Technology staff on March 27, 2009. The Office of Enterprise Security's response to our findings and recommendations are presented in the accompanying section of this report titled, *Agency Response*.

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

We would like to thank the staff from the Office of Enterprise Technology and all other agencies that participated for their cooperation during this audit.

/s/ James R. Nobles

James R. Nobles
Legislative Auditor

/s/ Cecile M. Ferkul

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

Small agencies in Minnesota state government generally do not have adequate security controls over their computer systems, which creates an unacceptable risk of unauthorized access to not public data and disruption to state functions. Effectively resolving these weaknesses is unlikely without the ongoing oversight and support of the Office of Enterprise Technology. This report contains six findings concerning control weaknesses in small agencies' computer systems.

Audit Objective and Scope

The primary objective of our audit was to answer the following question:

- Do small agencies have adequate controls to protect the integrity, confidentiality, and availability of their computer systems and data?

To answer this question, we assessed security controls at 12 small state agencies as of January 2009.

Background

We identified 45 small state agencies, which we defined as any office, bureau, board, commission, or agency with 50 or fewer employees. All of these agencies perform some service or function specified in state law. These agencies need to have secure computer systems to protect the state from financial losses and unauthorized disclosure of not public data; they need to have effective internal controls to address their information technology risks.

Overview

Small state agencies often use the same types of information technologies and are required to safeguard the same types of not public data as larger agencies. Therefore, small agencies need to have secure computer systems to protect the state from financial losses and unauthorized disclosure of not public data. They need to have effective internal controls to address their information technology risks.

We identified 45 small state agencies, which we defined as any office, bureau, board, commission, or agency with 50 or fewer employees. All of these agencies perform some service or function specified in state law.

Small agencies manage their information technology either with in-house staff or by using vendors to manage aspects of their technology and security. For example, some agencies use the state's Office of Enterprise Technology to provide firewall services or desktop computer support services.

The Office of Enterprise Technology has the responsibility to develop an enterprise approach to securing government computer systems and data. It has developed a security governance framework, a state enterprise security strategic plan, and several security-related policies. The office provides security expertise to state agencies. It is also implementing an enterprise-wide vulnerability assessment program.

Objectives, Scope, and Methodology

The primary objective of this information technology audit was to answer the following question:

- Do small state agencies have adequate controls to protect the integrity, confidentiality, and availability of its computer systems and data?

To answer this question, we examined controls at the following 12 small agencies:

Sample of Small Agencies	
Board of Accountancy	Office of Ombudsperson for Families
AELSLAGID[1]	Board of Pharmacy[2]
Council on Asian-Pacific Minnesotans	Public Utilities Commission
Board of Chiropractic Examiners[2]	Racing Commission
Gambling Control Board	Sentencing Guidelines Commission
Board of Nursing[2]	Workers' Compensation Court of Appeals

[1]AELSLAGID is the Minnesota Board of Architecture, Engineering, Land Surveying, Landscape Architecture, Geoscience, and Interior Design.

[2]One of 17 health-related licensing boards that jointly fund an administrative services unit to provide services, including information technology and security.

At each agency, we interviewed staff and reviewed policies, procedures, or other relevant documentation. We also interviewed staff at the Office of Enterprise Technology and reviewed relevant enterprise security policies. Finally, we used a variety of computer-assisted auditing tools to analyze the security infrastructure.

We conducted this audit in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. To assess security controls, we used criteria contained in the *Control Objectives for Information and Related Technology*,[1] published by the IT Governance Institute. We used criteria obtained from *Special Publications*, published by the National Institute of Standards and Technology's Computer Security Division.[2] We also used relevant policies and procedures to obtain evaluation criteria. Finally, we used information published by applicable technology vendors to evaluate select controls.

This information technology audit included a review of security data that the Minnesota Data Practices Act legally classifies as nonpublic. To protect state resources and comply with the Act, we withheld specific security-related details from this publicly released report. We communicated all pertinent details to the management of each agency in a separate, not public document.

[1] *Control Objectives for Information and Related Technology* is an IT governance framework providing organizations with a set of generally accepted measures, indicators, processes, and best practices to assist them in developing appropriate IT governance and control in an organization.

[2] The National Institute of Standards and Technology is a nonregulatory federal agency within the U.S. Department of Commerce. Its Computer Security Division responds to the Federal Information Security Management Act of 2002. *Special Publications* used included SP800-40 version 2 (Creating a Patch and Vulnerability Management Program), SP800-41 (Guidelines on Firewalls and Firewall Policy), SP800-77 (Guide to IPsec VPNs), SP800-92 (Guide to Computer Security Log Management), and 800-35 (Guide to Information Technology Security Services).

Conclusion

Small agencies in Minnesota state government generally do not have adequate security controls over their information systems, which creates an unacceptable risk of unauthorized access to not public data and disruption to state functions. Effectively resolving these weaknesses is unlikely without the ongoing oversight and support of the Office of Enterprise Technology. The following *Findings and Recommendations* section provides more detail about common control weaknesses in small agencies' computer systems.

Findings and Recommendations

Finding 1

Most small agencies did not have the necessary skills or financial resources to adequately manage and secure their computing environments.

Most small agencies we tested lacked sufficient financial resources to have staff dedicated to the management and security of their computing environments or to contract for adequate services from the Office of Enterprise Technology or another vendor.[3] As a result, the agencies were generally unaware that there were serious security weaknesses that exposed their computer systems and data to unauthorized access or disruption.

Seven of the twelve entities we audited did not have any dedicated full-time information technology or security staff. Some entities relied on staff without specialized training in computer technology, such as an attorney or a management analyst, to maintain their networks and computer equipment. Some agencies contracted with vendors to install and configure new technologies. Once installed, responsibility for ongoing management and maintenance rested with the agency. In most cases, the security controls were undocumented and poorly understood, resulting in controls diminishing significantly over time.

Information technology and security requirements are continually changing. It is not reasonable to expect that nontechnical staff will be able to keep up with this changing environment and adequately protect a small agency's systems. Also, state-of-the art security technologies can be expensive and cost prohibitive for any one small agency. Because a security breach at a small agency could expose the state to significant liability or expose other government computer systems to unauthorized access, the state needs to find ways to help small agencies better secure their computing environments. Effectively resolving the findings discussed in this report is unlikely without the ongoing oversight and support of the Office of Enterprise Technology.

[3] The boards of Pharmacy, Nursing, and Chiropractic Examiners included in our testing are three of seventeen health-related licensing boards that jointly fund an administrative services unit to provide services, including information technology and security. Because they pooled their resources and skills, these health-related boards generally had better controls than the other small agencies we reviewed.

Recommendation

- *The Office of Enterprise Technology should explore ways to help small agencies establish and maintain secure computing environments.*

Finding 2

Most small agencies did not sufficiently assess their technology risks, did not have written security policies, and did not have written agreements with vendors.

The majority of small agencies had not conducted risk assessments or developed formal written security policies, standards, procedures, and guidelines. In addition, some agencies did not have service level agreements with vendors who provided information technology services.

Periodic risk assessments are important because they help to identify, quantify, and prioritize risks. The results help to determine the appropriate management action and priorities for managing information security risks and for implementing controls selected to protect against these risks. Written policies, procedures, and standards outline management's security expectations and methods to fulfill those expectations. Staff or contractors cannot make consistent security decisions without policies and standards to refer to as guidance.

Agencies that obtained information technology services from vendors, including the Office of Enterprise Technology, often did not have formal service level agreements that included security services and responsibilities. Service level agreements are negotiated, formal agreements that stipulate the provided services, priorities, responsibilities, guarantees, and warranties. Some agencies thought they were receiving security-related services when they were not.

Recommendations

- *Agencies should periodically assess their information technology security risks and determine whether they need to make changes to their strategies to mitigate those risks.*

- *Agencies should develop written information technology security policies, standards, procedures, and guidelines.*

- *Agencies should negotiate formal service level agreements with vendors who provide information technology services.*

Finding 3

Small agencies did not have strong firewall controls to protect their systems from external threats and did not adequately segment their internal networks.

One agency did not have a firewall; another agency did not know whether it had a firewall because it obtained networking services through another state entity. The remaining agencies had firewalls, but weaknesses in the firewall setup exposed them to undue risk. Agencies had not documented firewall rules, including rule requests, approvals, and business justification. Agencies also did not periodically review and recertify firewall rules. As a result, agencies could not explain some rules and had some rules that were not needed or were too permissive.

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

The majority of agencies also did not use firewalls or devices to segment computers in their internal private network and filter computer traffic. Internal network segmentation improves control by only allowing authorized traffic in or out of each segment. Without internal segment protections, someone who accessed the internal private network could move freely throughout the network and attempt to access any computer and computer program on it. For example, anyone connected to the network could attempt to access powerful programs that only administrators need to access. Segmentation also helps prevent the spread of malicious software and viruses.

Recommendations

- *Agencies should document firewall rule requests, approvals, and business justification.*
- *Agencies should periodically review and recertify firewall rules.*
- *Agencies should segment their internal private networks and filter traffic between segments.*

Finding 4

Many small agencies lacked strong password controls.

Some small agencies did not configure computers to enforce strong password controls. Other agencies implemented security features, but permitted some accounts to circumvent those controls. Strong password controls are critical because they help prevent hackers from assuming the identity of legitimate system users. Most computer systems have customizable features to enforce strong password controls. For example, features can prevent users from selecting easy to guess passwords, like dictionary words, and requiring passwords to be periodically changed.

In addition, one agency did not change four default passwords belonging to extremely powerful database accounts on a purchased software product. Many purchased software products have default user accounts and passwords, and these are easily obtained from Internet websites. Immediately changing default passwords is essential to prevent a hacker from gaining unauthorized access.

Recommendation

- *Agencies should configure their computers to enforce strong password controls and change default passwords on their purchased software products.*

Finding 5

Most small agencies did not promptly install software updates or security-related software patches on some of its computers, and many computers were running unnecessary and insecure services or software.

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

Some computers were running unnecessary and insecure software or services. We identified many services on agency computers that were not necessary. The term “service” refers to a computer program that runs continuously, listening for specific commands. Services typically operate by default after installing a

computer operating system or other software and are needed to perform basic functions. 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.

Recommendation

- *Agencies should regularly install software patches and limit software and services to those that are authorized and necessary.*

Finding 6

Small agencies did not develop comprehensive security monitoring procedures and did not routinely scan their systems for common security vulnerabilities.

None of the small agencies we audited had developed comprehensive monitoring procedures to detect and promptly respond to security-related events, such as unauthorized attempts to access computer systems and data. In addition, most agencies did not run vulnerability assessment software to search for commonly known security weaknesses.

Although the best security controls are those that prevent inappropriate events from happening, it is virtually impossible to design flawless preventive defenses. This inherent security administration problem is why every organization must vigilantly monitor its systems for signs of attack. Since time is of the essence when under attack, every organization also must have predefined incident response procedures. Agencies that do not have effective procedures may fail to discover the security breach until after someone has gained unauthorized access and compromised its systems and data.

Agencies can customize software products to log various types of security events. Many software products can even send alerts to specific individuals when events occur. However, agencies did not assess its risks and define specific events to log and review. In addition to external attacks, other events require monitoring, such as system misuse by employees, changes to critical computer settings, and exceptions to defined policies and procedures.

Finally, most agencies did not run vulnerability assessment software to search for commonly known security weaknesses. Vulnerability scanners are special software packages that probe systems to find exploitable security weaknesses. An example of one such weakness is a bug in a commercial software product that could force a computer program to perform an unauthorized operation. Vendors that sell vulnerability scanners update their products frequently to include the most recent security exploits. Since hackers often take advantage of these exploits, it is important to find and correct them as quickly as possible. Had

agencies performed periodic vulnerability scans, it could have identified and corrected several of the security weaknesses that we found during our audit.

Recommendations

- *Agencies should define specific events to log and regularly review those logs to identify potential breaches or system misuse by employees.*

- *Agencies should routinely scan their computer systems for common security weaknesses.*

April 6, 2009

Mr. James Nobles, Legislative Auditor
Office of the Legislative Auditor
658 Cedar Street
Saint Paul, MN 55155

Dear Mr. Nobles:

I would like to thank your team for the work done on this audit of small agency security controls. We appreciate that you took the time to look beyond the specific technical problems in these small agencies to shed light on the bigger picture of what must be done to address the state's security challenges more holistically.

We agree with your overall conclusion: small agencies lack fundamental security controls. However, before responding to the specific findings in this report, it is important to emphasize that the security challenges that we face today go well beyond small agencies. Medium and large agencies also struggle to address increasingly complex cyber security threats, a fact that has been pointed out time and time again in other Legislative Audit reports.

It is clear is that the historical strategy of addressing cyber security threats on an agency by agency basis was not effective, and never will be. That is why our new Enterprise Security Program is developing centralized security solutions that can be shared by all agencies, and hopefully other levels and branches of government too. For example, with our security appropriation we are building a state-of-the-art solution that gives every agency and MnSCU campus the ability to continuously assess all computers for exploitable security vulnerabilities, an issue discussed in Finding 6. Before the rollout of our new Enterprise Vulnerability and Threat Management System, very few agencies had the people, processes, or tools to perform these vital functions.

It is also important to stress that the State of Minnesota's decentralized information technology environment is inherently difficult to secure. The findings in this report point to the fact that information technology operations must be supported by skilled security professionals and sophisticated technologies that operate around the clock. The brutal reality that we must accept is that it simply will not be possible to operate over 36 government data centers with the necessary physical and technical security controls, unless we are prepared to spend considerably more. The Executive Branch has been working to consolidate its data centers into one highly-secure primary facility with a secondary facility for disaster recovery. This will help us simplify our technology architecture and implement more cost effective physical and technical security controls for the entire government.

Finding 1

Most small agencies did not have the necessary skills or financial resources to adequately manage and secure their computing environments.

Recommendation

- *The Office of Enterprise Technology should explore ways to effectively and efficiently help small agencies establish and maintain secure computing environments.*

Office of Enterprise Technology Response

We concur with both the finding and recommendation.

With our security appropriation, we are doing what we can to help agencies without dedicated security professionals. For example, we designated two individuals to serve as security leads for agencies that do not have their own security staff.

In addition, as we develop central security solutions, we also are working to extend those solutions to smaller organizations. For example, we are developing a special version of the Enterprise Vulnerability and Threat Management System for small and medium sized organizations. The powerful security appliances that are part of the Enterprise Vulnerability and Threat Management System are prohibitively expensive to deploy in smaller agencies. Our custom solution will let multiple agencies share the capacity of expensive devices.

The actions that we are taking today to help secure small and medium sized agencies are important stop gap measures. However, long-term we will need to abandon our decentralized security model if we ever hope to overcome the two fundamental issues in the finding statement:

1. Agencies do not have the necessary **skills**; and
2. Agencies do not have the necessary **financial resources**.

Our solution to address these two underlying issues is to move to a more centralized technology management model. Consolidating the state's data centers is an important first step.

Finding 2

Most small agencies did not sufficiently assess their technology risks, did not have written policies, and did not have written agreements with vendors.

Recommendations

- *Agencies should periodically assess their information technology security risks and determine whether they need to make changes to their strategies to mitigate those risks.*

- *Agencies should develop written information technology security policies, standards, procedures, and guidelines.*

- *Agencies should negotiate formal service level agreements with vendors who provide information technology services.*

Office of Enterprise Technology Response

We concur with the finding and agree that the recommendations are valid approaches to address the underlying issues. However, we do not think that many of these agencies possess the necessary skills or resources to implement the recommendations. As stated in Finding 1, seven of the twelve entities included in the scope of this audit did not have any full-time information technology or security staff. Also, most entities had undocumented and poorly understood controls that degraded over time due to inattention. Entities should not be in the business of managing technology if they cannot deploy and sustain appropriate security controls, which is why we are recommending a centralization strategy.

Finding 3

Small agencies did not have strong firewall controls to protect their systems from external threats and did not adequately segment their internal networks.

Recommendations

- *Agencies should document firewall rule requests, approvals, and business justification.*

- *Agencies should periodically review and recertify firewall rules.*

- *Agencies should segment their internal private networks and filter traffic between segments.*

Office of Enterprise Technology Response

We concur with the finding and agree that the recommendations are valid. However, managing a firewall is complex and requires very specialized skills so it may be difficult for agencies to independently implement these recommendations given their resource limitations.

Finding 4

Most small agencies lacked strong password controls.

Recommendation

- *Agencies should configure their computers to enforce strong password controls and change default passwords on their purchased software products.*

Office of Enterprise Technology Response

We concur with the finding and agree that the recommendation is valid. However, we think that a more effective strategy will be to alleviate small agencies of these duties altogether. Moving towards a central management model will put information technology professionals in charge of complex security administration duties and will free up agency staff to fulfill their business missions.

Finding 5

Most small agencies did not promptly install software updates or security-related software patches on some of its computers, and many computers were running unnecessary and insecure services or software.

Recommendation

- *Agencies should regularly install software patches and limit software and services to those that are authorized and necessary.*

Office of Enterprise Technology Response

We concur with the finding and agree that the recommendation is a valid approach to address the underlying issue. However, the types of server hardening and security management tasks outlined in the finding require special skills and tools that small agencies will never possess. A more effective strategy will be to alleviate small agencies of these duties altogether and move towards a central management model.

Finding 6

Small agencies did not develop comprehensive security monitoring procedures and did not routinely scan their systems for common security vulnerabilities.

Recommendations

- *Agencies should define specific events to log and regularly review those logs to identify potential breaches or system misuse by employees.*

- *Agencies should routinely scan their computer systems for common security weaknesses.*

Office of Enterprise Technology Response

We concur with the finding and agree that the recommendations are valid. However, in order to implement these recommendations it is important that agencies have both powerful centrally managed tools and a hands-on assistance. For example, the Office of Enterprise Technology is now deploying a special version of the Enterprise Vulnerability and Threat Management System for small agencies. This powerful tool will give small agencies the ability to schedule and manage their own vulnerability assessments, although powerful tools alone will provide little value to organizations that do not have skilled technical staff. Consolidating state data centers and moving towards a more centralized technology management model will help the Office of Enterprise Technology provide badly needed security services more cost effectively.

Once again, I want to thank you for the opportunity to respond to the audit findings. If you have any questions regarding our response, please do not hesitate to contact me.

Sincerely,

/s/ Gopal Khanna

Gopal Khanna
Chief Information Officer