OLA

OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA

FINANCIAL AUDIT DIVISION REPORT

Vulnerability Management

Information Technology Audit

For the Period July 2010 to July 2011

May 22, 2012 **Report 12-11**

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

May 22, 2012

Representative Michael Beard, Chair
Legislative Audit Commission

Members of the Legislative Audit Commission

Carolyn Parnell, State Chief Information Officer
Office of Enterprise Technology

This report presents the results of our information technology audit of the state's vulnerability management process for the period of July 2010 to July 2011. This report contains four findings presented in the accompanying section of this report titled, Findings and Recommendations.

We discussed the results of the audit with the staff of the Office of Enterprise Technology on May 7, 2012. The office's response to our findings and recommendations is presented in the accompanying section of this report titled, Agency Response.

The audit was conducted by Carolyn Engstrom, CISA (Audit Manager); Bill Betthauser, CISA; and David Westlund, CPA CISA.

This report is intended for the information and use of the Legislative Audit Commission and the management of Office of Enterprise Technology. This restriction is not intended to limit the distribution of this report, which was released as a public document on May 22, 2012.

We received the full cooperation of the Office of Enterprise Technology's staff and other state agencies' information technology 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 Office of Enterprise Technology established internal controls that were generally adequate to identify and resolve security vulnerabilities; however, the office had not adequately communicated some parts of its vulnerability management standard, and training materials did not address all requirements of the standard.

The state did not comply with the Enterprise Vulnerability Management Security Standard. Agencies had generally not classified the criticality of devices (computers, systems, and networks) based on the confidentiality, integrity, and availability requirements of their data, as required by the standard. Also agencies did not consistently report certain events to the Office of Enterprise Technology, and some agencies did not effectively conduct scans and prioritize the remediation of their vulnerabilities. The Office of Enterprise Technology also did not provide state agencies with certain metrics related to agencies' device criticality, as required by the standard.

Findings

- Agencies have not assigned vulnerability ratings to devices based on the requirements of the data and systems they support. (Finding 1, page 7)
- Some agencies did not have complete, effective, or efficient internal scanning practices and did not report scanning policy exceptions to the Office of Enterprise Technology. (Finding 2, page 9)
- Agencies had not adequately resolved vulnerabilities identified by system scans. (Finding 3, page 11)
- While the Office of Enterprise Technology provided various training sessions to agency information technology staff about specific aspects of the vulnerability management program, the office did not develop a comprehensive and role-based training curriculum. (Finding 4, page 13)

Audit Objective and Scope

The audit objective was to answer the following questions for the period from July 1, 2010, through July 31, 2011:

- Did the Office of Enterprise Technology's Vulnerability Management Security Standard establish adequate internal controls to manage vulnerabilities of the state's computers, systems, and networks?
- Did the Office of Enterprise Technology and the state agencies comply with the Enterprise Vulnerability Management Security Standard?

Vulnerability Management

Overview

Vulnerability management is an information technology process aimed at identifying and mitigating weaknesses in operating systems, applications, and communication protocols. Unmitigated vulnerabilities provide ways for hackers to attack a system in order to deny access to a system for legitimate users, use a compromised device to attack another system, or steal data. The National Institute of Standards and Technology asserts that a proactive vulnerability management process requires considerably less time and effort than is required to respond to a systematic attack or data breach.[1] A preemptive approach is still challenging because of the number and sophistication of vulnerabilities is growing. Computer security experts identify thousands of new vulnerabilities each year.[2]

Historically, state agencies approached vulnerability management independently. Some agencies had actively scanned computers and servers on their networks to identify and mitigate vulnerabilities; others, to varying degrees, had not. Without a consistent tool, strategy, or approach across agencies, the state could not comprehensively assess its vulnerabilities or the effectiveness of agencies' efforts to mitigate their risks in a timely manner. In 2006, the newly created Office of Enterprise Technology considered unidentified and unmitigated vulnerabilities to be a high risk to the security of the state's computer systems, networks, and data.

In 2007, the Office of Enterprise Technology contracted with a vulnerability management vendor for a tool to scan state computer hardware and networks to identify and report vulnerabilities. The office made the tool available to agencies and began to develop a vulnerability management program, which included drafting a statewide standard for vulnerability management and establishing a vulnerability and threat management team to train and assist agency staff. The office, in conjunction with representatives from state agencies, approved an Enterprise Vulnerability Management Security Standard in December 2009, which stipulated that agencies be compliant by December 2010.[3] Table 1 summarizes the elements of the standard.

[1] National Institute of Standards and Technology, Special Publication 800-40, page 1-2.
[2] Computer Emergency Response Team (CERT) studies internet security vulnerabilities. Statistics about vulnerability trends is available at its website - http://www.cert.org/stats/.
[3] The Enterprise Vulnerability Management Security Standard is located on the Office of Enterprise Technology's Information Security Policies and Standards web page: http://mn.gov/oet/policies-and-standards/information-security/#

Table 1
Vulnerability Management Program Steps

Initialize and Configuration: Identify the networks to be scanned and teams responsible for vulnerability management.

Asset Discovery: Establish a complete inventory of devices[4] and conduct a criticality impact assessment based on the confidentiality, integrity, and availability requirements of the information the device processes or stores and how accessible the device is from the internet. Assign a criticality rating (critical, high, medium, or low) to the device or network in the scanning tool.

Vulnerability Scanning: Configure scans according to the standard scanning requirements established by the Office of Enterprise Technology and conduct the scans on a schedule (weekly, monthly, quarterly) determined by the criticality rating. Scan results contain information about the host that was scanned, the vulnerability that was identified, the vulnerability's score (based on proprietary calculations), and the risk posed by the vulnerability (such as gaining remote or local administrative access), as well as potential remediation solutions.

Vulnerability Analysis and Prioritization: Confirm that scan results include only valid vulnerabilities and that the score assigned to the vulnerability properly reflects the risk it presents.

Vulnerability Resolution: Mitigate the risk the vulnerability presents, applying a patch for example, within the prescribed timeframe based on the vulnerability's score and the criticality impact rating of the device at risk.

Resolution Confirmation: Confirm that the vulnerability was remediated through patching or that other controls designed to mitigate the risk of the vulnerability are operating effectively.

Vulnerability Reporting: Agencies communicate excluded networks and/or devices and falsely identified vulnerabilities to the Office of Enterprise Technology's vulnerability management team. The Office of Enterprise Technology generates metrics to communicate the level of agency compliance with the enterprise vulnerability standard.

Source: Auditor created based on the Office of Enterprise Technology's Enterprise Vulnerability Management Security Standard.

[4] A device is any piece of computing equipment that can be assigned an internet protocol address, such as a server, laptop, desktop computer, smartphone, router, switch, tablet, or wireless access point, etc.

During its 2011 Special Session, the Legislature passed a law[5] which reassigned information technology employees of state agencies to of the Office of Enterprise Technology, under the direction of the State Chief Information Officer. It is unclear how this structural change will impact the state's vulnerability management strategies. Although the responsibility for the management and operation of the state's computer systems and networks has shifted from the state agencies to the Office of Enterprise Technology, the business operations and data supported by those systems and networks remain the responsibility of the state agencies. While identifying and addressing vulnerabilities that pose risks to the state's systems and networks is an information technology responsibility, it is the state agencies' determinations of the criticality of the business operations and data that should dictate how often to scan for vulnerabilities and how quickly to resolve them. Vulnerability management will continue to require coordination and cooperation between the Office of Enterprise Technology and state agencies.

Objective, Scope, and Methodology

The audit objective was to answer the following questions for the period from July 1, 2010, through July 31, 2011:

- Did the Office of Enterprise Technology's Vulnerability Management Security Standard establish adequate internal controls to manage vulnerabilities of the state's computers, systems, and networks?

- Did the Office of Enterprise Technology and the state agencies comply with the Enterprise Vulnerability Management Security Standard?

To answer these questions, we:

- Gained an understanding about the state's vulnerability management strategy, interviewed staff from the Office of Enterprise Technology and technology staff at selected state agencies; reviewed relevant documentation, including the office's Vulnerability Management Security Standard; and surveyed state agencies about their implementation of the standard.

- Assessed how effectively the state was using the vulnerability scanning tool provided by the Office of Enterprise Technology by applying a variety of computer-assisted auditing tools and other techniques to analyze data about and resulting from vulnerability scans of agencies' computers, systems, and networks.

- Validated survey responses and determined whether state agencies complied with the state's vulnerability management policy and standard by performing more detailed tests and conducting in-depth interviews of

[5] *Laws of Minnesota* 2011, First Special Session, Chapter 10, Article 4, Section 2.

staff at eight agencies, selected based on their survey responses and our preliminary analysis of scanning data.[6]

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 Office of Enterprise Technology's Vulnerability Management Security Standard, and the National Institute of Standards and Technology's *Special Publication 800-40 (Creating a Patch and Vulnerability Management Program) and Special Publication 800-53 (Recommended Security Controls for Federal Information Systems).*

Conclusion

The Office of Enterprise Technology established internal controls that were generally adequate to identify and resolve security vulnerabilities; however, the office had not adequately communicated some parts of its vulnerability management standard, and training materials did not address all requirements of the standard.

The state did not comply with the Enterprise Vulnerability Management Security Standard. Agencies had generally not classified the criticality of devices (computers, systems, and networks) based on the confidentiality, integrity, and availability requirements of their data, as required by the standard. Also agencies did not consistently report certain events to the Office of Enterprise Technology, and some agencies did not effectively conduct scans and prioritize the remediation of their vulnerabilities. The Office of Enterprise Technology also did not provide state agencies with certain metrics related to agencies' device criticality, as required by the standard.

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

[6] We performed this additional testing at the following eight state agencies: Department of Human Services, Office of Enterprise Technology, Campaign Finance and Public Disclosure Board, Department of Revenue, Office of the State Auditor, Department of Corrections, Zoological Board, and Health Licensing Boards.

Findings and Recommendations

Agencies have not assigned vulnerability ratings to devices based on the requirements of the data and systems they support.

Finding 1

Many state agencies have not assessed or rated their devices based on the criticality of the confidentiality, availability, and integrity requirements[7] of the data the device processed or stored and how accessible the device was to the internet.[8] Of the 56 agencies that responded to our survey, 26 stated that they had not formally assessed the criticality of specific devices, and 19 stated that they had partially completed an assessment. Our analysis of the state's vulnerability data, as of July 2011, indicated that 14 agencies had entered criticality ratings[9] for at least 90 percent of their devices in the scanning tool. Of those 14 agencies, 11 were small agencies that provided a criticality rating for their entire network. Some agencies had not entered a criticality rating in the scanning tool but may have formally or informally assessed their devices. Other agencies entered a criticality rating in the tool that was not based on a formal or informal assessment.

The state's Enterprise Vulnerability Management Security Standard required agencies to assess their devices to determine their criticality rating, and it provided a high level methodology to perform the assessment, as shown in Table 2. Additionally, the office conducted training in April 2011, providing examples of assessments of various kinds of devices and explaining how to record the values in the scanning tool.

Overall compliance with the standard depends on agencies adequately completing a criticality impact assessment and assigning criticality ratings to devices and/or networks. The standard uses the criticality rating as a basis for an agency to determine how often it should scan a device and, in conjunction with the tool's vulnerability score, how quickly it should remediate a vulnerability. Because agencies had not complied with this fundamental requirement of the standard, they were unable to demonstrate that scan schedules correlated to the criticality of the devices. In addition, by entering criticality ratings into the scanning tool, agencies could create reports that more effectively identify high risk vulnerabilities, helping them to better prioritize their remediation efforts.

---

[7] Confidentiality, integrity, and availability are the terms used in the information technology community to describe the core objectives of information security. The objective of confidentiality is that the system's security will ensure that only authorized persons will have access to information. The classification of the information determines the degree of confidentiality required and the appropriate safeguards. *Minnesota Statutes* 2011, Chapter 13, Government Data Practices, classifies government data into the following categories: public, confidential, private, nonpublic, or protected nonpublic.

[8] A device is any piece of computing equipment that can be assigned an internet protocol address, such as a server, laptop, desktop computer, smartphone, router, switch, tablet, or wireless access point, etc.

[9] For purposes of this report, criticality impact assessment refers to the process of determining a rating for a device. The Office of Enterprise technology referred to the criticality rating as the "exposure criticality" and "asset exposure" in the standard.

Table 2
Vulnerability Classifications
Based on Device Impact Rating and Vulnerability Risk Exposure

	Risk Exposure			
Impact Rating:	Stand-alone system with limited or no network connectivity	System with network visibility is limited to local network	System with network visibility is available to MNET or broader audience (not internet facing)	System visibility is available from the internet
HIGH IMPACT: **Confidentiality:** System contains not public data. **Availability**: System must be available at all times. **Integrity:** System transmits, processes, or stores important data that may be used to make significant business decisions.	MEDIUM	HIGH	CRITICAL	CRITICAL
MODERATE IMPACT: **Confidentiality:** System contains data with an unknown classification. **Availability**: System can experience some down time or limited availability outside of normal business hours. **Integrity**: System contains data that is important to the business function of the agency.	LOW	MEDIUM	HIGH	CRITICAL
LOW IMPACT: **Confidentiality:** System does not contain not public data. **Availability**: System can experience extended down time, or no availability required outside of normal business hours. **Integrity:** Does not transmit, process, or store data that is important to the business function of the agency.	LOW	LOW	MEDIUM	HIGH

Source: Office of Enterprise Technology's Enterprise Vulnerability Management Security Standard, Appendix A.

In preparing its monthly analysis of how effectively agencies used the scanning tool, the Office of Enterprise Technology, in accordance with the standard, considered any device that did not have a criticality rating in the tool to have a rating of "high." As a result, the analysis may have overstated the number of unresolved high-priority vulnerabilities; the analysis generally showed that most agencies were not effectively remediating high priority vulnerabilities within the timeframes required by the standard.

The Office of Enterprise Technology produced monthly analysis reports that measured agencies' performance on many operational and compliance-related aspects of the standard, such as percent of devices scanned within seven days, percent of devices scanned with credentials, and percent of priority vulnerabilities resolved within required timeframes. However, the office's monthly analysis reports did not include a tally of devices by their criticality rating (low, medium, high, and critical), the number and percentage of devices scanned by criticality rating, or the percentage of assets scanned in accordance with the criticality scan frequency set by the standard, which are specified in the vulnerability management standard.

Recommendations

- *Agencies should conduct a criticality impact assessment to determine the criticality rating of their devices based on the requirements of the data stored or processed by devices.*
- *Agencies should work with the Office of Enterprise Technology to record the criticality ratings in the state's vulnerability scanning tool.*
- *Agencies should use the criticality ratings to determine whether they have complied with or exceeded the scan frequency requirements of the standard.*
- *The Office of Enterprise Technology should develop and communicate device criticality metrics required by the vulnerability management standard.*

Finding 2

Some agencies did not have complete, effective, or efficient internal scanning practices and did not report scanning policy exceptions to the Office of Enterprise Technology.

Agency system administrators had not documented the basis for making scan exclusions, assessed the need for additional controls to mitigate the risks created by the scan exclusion, or reported to the Office of Enterprise Technology's vulnerability and threat management team devices or networks that they had excluded from vulnerability scanning. The vulnerability standard requires agencies to scan all devices and networks, unless there is a valid reason for an exclusion.[10] Agencies' responses to our survey and subsequent analysis of scanning tool data identified the following deficiencies in agencies' scanning practices:

- Four small agencies were not scanning their external and internal networks.

[10] Valid reasons to exclude certain devices would include scans causing certain servers to become unresponsive, or the device may not be connected to the network and is under adequate physical control.

- Two of these agencies were working with the Office of Enterprise Technology to implement scans.
- One agency was using other third party tools to perform vulnerability scanning. They did not intend to transition to the state's scanning tool.
- The remaining agency's network was believed by the office to be included in a separate agency's scan, but was subsequently determined to not be included in the state's external network scans.

- Seven agencies were not scanning some devices on their internal networks, and six agencies were not scanning some of their internal networks.
- One agency was in the process of transitioning to the state's vulnerability management scanning tool from its own scanning tool.
- Many small agencies that contracted with the Office of Enterprise Technology for vulnerability scanning assumed, but did not know if, all devices and all networks were being scanned.
- One agency was scanning only one of its seven internal networks; neither the agency nor the Office of Enterprise Technology was aware of this deficiency.
- Agencies were required by the standard to inventory all devices that generated, processed, transmitted, or stored government data. However the standard did not define what elements must be included in the inventory or how that information should be used. When agencies maintain an inventory independent of the data in the scanning tool, they can compare their inventory to scan results to ensure that all networks and devices are being scanned.
- The standard required agencies to have "action plans" to establish the approach to remediating a vulnerability; however, the standard did not describe the elements to be included in an action plan or provide guidance in how to document an action plan.

Some agencies were not conducting authenticated scans, as required by the standard whenever that type of scan was possible.[11] Authenticated scans involve providing privileged login credentials to the scanning tool so it can accurately determine the device's operating system and applications installed on the device to produce more specific vulnerability results. Eight agencies were not performing any authenticated scanning. Five agencies were performing authenticated scanning on less than 10 percent of their devices.

[11] Some operating systems and certain other circumstances may prevent the use of authenticated scans.

Recommendations

- *Agencies should ensure the completeness of the scanning process and the authorization of any devices excluded from the process. The Office of Enterprise Technology should provide state agencies with more specific direction about how to comply certain elements of the standard, including requirements related to device inventories and vulnerability action plans.*

- *Agencies should conduct authenticated scans of their networks and devices whenever possible.*

Finding 3

Agencies had not adequately resolved vulnerabilities identified by system scans.

Agencies had not adequately resolved vulnerabilities identified through the scanning process, as directed in the standard.[12] Agency staff can resolve vulnerabilities in several ways, including applying an update or patch provided by a vendor, making changes to an operating system, removing an unauthorized or insecure application, or by isolating and restricting access to an application. Agencies had the following challenges in identifying and resolving high-priority vulnerabilities:

- Because the Office of Enterprise Technology defaulted to a high criticality rating for any devices without a criticality rating in the scanning tool, the office's metrics considered many of the resulting vulnerabilities identified by the scanning tool to be high or critical vulnerabilities. The standard expected agencies to resolve these high-priority vulnerabilities within one to six weeks; however, most agencies did not achieve this target.

- Prior to June 2010, agencies had a limited ability to query the scanning data to create customized reports. As of June 2010, the state implemented a tool to allow agencies to create more customized reports.

- The Office of Enterprise Technology had purchased hardware to build a vulnerability data warehouse and created some customized reports, but had not provided agencies with access to the data or the customized reports. For example, the office had created a report to identify new vulnerabilities since the last scan; however, the office had not distributed the report to all agencies.

[12] Enterprise Vulnerability Management Security Standard, Phase E, page 5.

- The scanning tool continued to report vulnerabilities even though the agency had mitigated the risk posed by the vulnerability through some method other than patching.

- Agencies had not resolved a backlog of vulnerabilities that accumulated since agencies began scanning their networks. Because each new scan identified new vulnerabilities, agency staff was challenged to both address new high-risk vulnerabilities and reduce the backlog of vulnerabilities previously identified.

- Through the survey, 19 agencies reported that they did not have a process to sign off and accept the risk of vulnerabilities that they could not remediate. Only one vulnerability was signed off by agency management and reported to the office.

- Agencies were generally unaware of how to determine whether a vulnerability the scanning tool identified was valid and how to report invalid vulnerabilities to the Office of Enterprise Technology. The complexities of vulnerability scanning can result in false positives – an indication that a vulnerability exists when it does not. The standard did not explain how to validate vulnerabilities or how to report false positives to the Office of Enterprise Technology. As a result, agencies reported false positives inconsistently; sometimes via telephone, email to the vulnerability and threat management team, or submission of a service desk ticket. Reporting false positives to the office allows the office to adjust the scanning tool to reduce the occurrence of false positives on future scans.

While patching is not the only way to remediate vulnerabilities, it tends to be one of the most common. The state's vulnerability scanning tool identifies vulnerabilities but does not help agencies patch them. Many agencies obtained specialized software to apply vendor supplied patches to numerous computers. Through our survey, state agencies identified at least nine different software applications used to remediate vulnerabilities. Some agencies, primarily smaller ones, did not use any specialized patching software. The Office of Enterprise Technology could provide more consistent guidance about remediation if state agencies used the same patching software.

Recommendations

- *Agencies should establish milestone dates to clear their backlog of vulnerabilities based on the criticality exposure of the devices.*

- *Agencies should report false positives to the vulnerability and threat management team in a timely and consistent manner.*

- *The Office of Enterprise Technology should designate a remediation patching software.*

- *Agencies should collaborate with the Office of Enterprise Technology to ensure that adequate reporting is available from the state's scanning tool.*

Finding 4

While the Office of Enterprise Technology provided various training sessions to agency information technology staff about specific aspects of the vulnerability management program, the office did not develop a comprehensive and role-based training curriculum.

The Office of Enterprise Technology did not adapt its training to meet the needs of different staff roles involved in the vulnerability management process. For example, server administrators, desktop administrators, and network administrators need to understand how to validate and remediate vulnerabilities. Chief information security officers need to understand how to prioritize vulnerabilities, track vulnerabilities for remediation, retain documentation, and monitor metrics. Chief information officers need to understand metrics and how to direct the activities of information technology staff. Also, because agencies experienced significant turn-over in information technology staff throughout the implementation of the vulnerability management program, they may have lost organizational knowledge.

Since 2007, the Office of Enterprise Technology provided many different types of training to a variety of audiences during implementation of the state's vulnerability management program. The vendor provided detailed, multiday training when the scanning tool was first implemented. The office has conducted numerous training sessions on aspects of policy, such as the April 2011 session on conducting critical impact assessment. The vulnerability management team frequently conducted presentations at statewide forums for the information technology community, and new users must attend training sessions prior to obtaining access to the scanning tool. In addition, the vulnerability management personnel are available for one-on-one training sessions at user requests.

However, the office did not integrate its various vulnerability management resources to make them easily available to agency staff. An agency employee would need to find and review the resources shown in Table 3 to understand the requirements of the vulnerability management program. Some of the resources were only available through secured websites or for those attending training sessions. Even with these resources, identifying the individual responsibilities and expectations of a role may be difficult to determine and vary from agency to agency.

Table 3
Resources Needed to Understand the State's Vulnerability Management Program and Where Those Resources are Available

Resource	Availability
Office of Enterprise Technology's Vulnerability Management Security Standard	Office of Enterprise Technology's public internet site
Vulnerability Management Program Training Document	Distributed to people who attended training
Description of Vulnerability Management Metrics	Located on a secured website
Training Manual for Vulnerability Management Tool	Located on a secured website
Training Presentation for Assigning Asset Values	Located on a secured website
NIST Special Publication 800-40 Creating a Patch and Vulnerability Management Program	Referred to in vulnerability management training documentation, available at NIST's Computer Security Resource Center
Enterprise Vulnerability Management Mitigation Report	In draft, not generally available

Source: Auditor created.

In addition, the new-user training required by the office did not reference the standard and did not provide adequate context for agencies to understand how certain settings in the tool helped the agency achieve compliance with the standard. For example, the training did not include the following information:

- Where agency staff could record in the scanning tool an asset's criticality rating.
- The requirement that agencies use authenticated scans, where possible.
- When and how the office would measure and report on state agency compliance with aspects of the standard, such as how timely agencies had resolved high-risk vulnerabilities.
- The additional reporting capabilities of the scanning tool that could assist the agency in achieving compliance with the standard.
- Ways that agencies needed to supplement the scanning tool to achieve compliance with the standard, such as the need to create action plans or to communicate certain information to the office.

Without a good understanding of the vulnerability management process and the state's specific requirements, it is unlikely the state will achieve wide-spread, consistent compliance to ensure that it adequately protects the confidentiality, integrity, and availability of its computers, networks, systems, and data. Further, even in an environment where training is timely, relevant, and effective and reference materials are readily available, agencies may assign a lower priority to complying with the vulnerability management standard and allocate information technology personnel to more pressing strategic initiatives. The consolidation of information technology employees under the Office of Enterprise Technology may provide an opportunity for the state to have a team of dedicated specialists focus on some specific, technical aspects of vulnerability management, rather than having these duties dispersed across state agencies.

Recommendation

- *The Office of Enterprise Technology should update training materials to provide a comprehensive understanding of the overall vulnerability management program. The training materials should address the responsibilities of different roles for ensuring compliance with elements of the vulnerability management standard.*

SERVICES

Central Office

May 17, 2012

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

Dear Mr. Nobles:

I and the Office of Enterprise Technology (MN.IT Services) team would like to thank your team for the work done on this statewide audit of vulnerability management controls. Our organization appreciates that you took the time to look at this vital security area from an enterprise-wide perspective and we agree with your overall conclusion that controls are generally adequate. But we also agree that much more can and should be done to further strengthen the security posture of executive branch agencies in the State of Minnesota.

We are extremely proud of our Enterprise Vulnerability Management Program, which is recognized as a model of excellence nationally. Each day, security professionals proactively assess thousands of executive branch and higher education computers to find and fix vulnerabilities before they are exploited. Our program is based on a solid policy and standard foundation that has been shared with and used by many other states, hoping to replicate what we have accomplished. Our policy and standard sets a very high bar because in a world that is fraught with cyber security risks, organizations need to find and fix security holes fast.

Your report accurately points out that agency security and technology professionals are not doing a good enough job remediating vulnerabilities promptly, as required by our policy and standard. Though the report directs many recommendations to agencies, we do not think that simply asking agencies to do more will yield different results. We believe that we must change our vulnerability management delivery model from a federated to a centralized model to avoid the same audit findings further down the road. IT consolidation sets the stage to deliver mission critical vulnerability management services centrally, with the rigor that is needed to meet the requirements in our state policy and standard.

The Office of Enterprise Technology
658 Cedar Street, Saint Paul MN 55155
www.mn.gov/oet

Finding 1: Agencies have not assigned vulnerability ratings to devices based on the requirements of the data and systems they support.

Recommendation

- *Agencies should conduct a criticality impact assessment to determine the criticality rating of their devices based on the requirements of the data stored or processed by devices.*
- *Agencies should work with the Office of Enterprise Technology to record the criticality ratings in the state's vulnerability scanning tool.*
- *Agencies should use the criticality ratings to determine whether they have complied with or exceeded the scan frequency requirements of the standard.*
- *The Office of Enterprise Technology should develop and communicate all device criticality metrics required by the vulnerability management standard.*

MN.IT Services Response

We concur with both the finding and recommendations.

We acknowledge that the State is not as mature as we'd like with classifying systems within our vulnerability management tool. We are, however, pleased that critical vulnerabilities are in fact being detected and remediated every day. Just a few years ago, virtually no agencies had processes or tools to identify security vulnerabilities in their technology environments.

When we developed our Enterprise Vulnerability Management Program, our top priorities were to 1) set a solid policy and standard foundation and 2) provide agencies with a state-of-the-art scanning tool to identify vulnerabilities. Focusing on these two priorities helped get agencies into a position where they could begin finding and fixing vulnerabilities before they were exploited by hackers.

Assigning criticality ratings to systems is an important next step. Without system criticality ratings, security professionals and technology administrators cannot use the scanning tool to its fullest potential to prioritize remediation efforts. While all critical vulnerabilities should be fixed, it is clearly most important to address security vulnerabilities on life/safety and other high priority systems first.

We believe that IT consolidation will provide us with better management control and oversight to resolve this finding. Agency-based Chief Information Officers (CIOs), together with our manager over vulnerability management, will implement process changes to resolve the audit finding. Resolution tactics, with anticipated milestone completion dates, will be included in our information security two-year tactical plan, due to be completed by July 1, 2012. Mark Mathison, our Information Security Manager over Governance, Risk and Compliance will oversee resolution efforts. We anticipate resolution to be completed by June 30, 2014.

Finding 2: Some agencies did not have complete, effective, or efficient internal scanning practices and did not report scanning policy exceptions to the Office of Enterprise Technology.

Recommendations

- *Agencies should ensure the completeness of the scanning process and the authorization of any devices excluded from the process. The Office of Enterprise Technology should provide state agencies with more specific direction about how to comply certain elements of the standard, including requirements related to device inventories and vulnerability action plans.*
- *Agencies should conduct authenticated scans of their networks and devices whenever possible.*

MN.IT Services Response

We concur with the finding and the recommendations, but believe that IT consolidation will change how the recommendations will be implemented.

Today, most agencies do not have the dedicated staff needed to focus on vulnerability management issues. With IT consolidation, an opportunity now exists to create a centralized team of dedicated and highly skilled vulnerability management professionals. This team will follow a consistent and repeatable methodology to make sure that problems get resolved in a timely manner and meet the requirements that are outlined in our policy and standard.

We believe that IT consolidation will provide us with better management control and oversight to resolve this finding. Agency-based Chief Information Officers (CIOs), together with our manager over vulnerability management, will implement process changes to resolve the audit finding. Resolution tactics, with anticipated milestone completion dates, will be included in our information security two-year tactical plan, due to be completed by July 1, 2012. Mark Mathison, our Information Security Manager over Governance, Risk and Compliance will oversee resolution efforts. We anticipate resolution to be completed by June 30, 2014.

Finding 3: Agencies had not adequately resolved vulnerabilities identified by system scans.

Recommendations

- *Agencies should establish milestone dates to clear their backlog of vulnerabilities based on the criticality exposure of the devices.*
- *Agencies should report false positives to the vulnerability and threat management team in a timely and consistent manner.*
- *The Office of Enterprise Technology should designate a remediation patching software.*
- *Agencies should collaborate with the Office of Enterprise Technology to ensure that adequate reporting is available from the state's scanning tool.*

MN.IT Services Response

We concur with the finding and the recommendations, but believe that IT consolidation will change how the recommendations will be implemented.

Today, most agencies struggle with competing priorities and do not have the dedicated staff to focus on vulnerability management issues. This often results in a backlog of remediation efforts. With IT consolidation, we plan to deliver vulnerability management services centrally with a dedicated team of security professionals. With a dedicated team and an extension of the processes now used in today in our central IT organization, we are confident that we will be able to significantly reduce the time that it takes to remediate vulnerabilities.

We believe that IT consolidation will provide us with better management control and oversight to resolve this finding. Executive management of MN.IT Services is ultimately accountable for the audit finding resolutions. Agency-level Chief Information Officers (CIOs), together with our manager over vulnerability management, will implement process changes to resolve the audit finding. Resolution tactics, with anticipated milestone completion dates, will be included in our information security two-year tactical plan, due to be completed by July 1, 2012. Mark Mathison, our Information Security Manager over Governance, Risk and Compliance will oversee resolution efforts. We anticipate resolution to be completed by June 30, 2014.

Finding 4: While the Office of Enterprise Technology provided various training sessions to agency information technology staff about specific aspects of the vulnerability management program, the office did not develop a comprehensive and role-based training curriculum.

Recommendation

- *The Office of Enterprise Technology should update training materials to provide a comprehensive understanding of the overall vulnerability management program. The training materials should address the responsibilities of different roles for ensuring compliance with elements of the vulnerability management standard.*

MN.IT Services Response

We concur with the finding and the recommendations.

As the audit noted, we took many steps to educate numerous individuals on vulnerability management strategies. We appreciate the feedback on how we can strengthen our program and will make efforts to implement your recommendations. As noted earlier, we believe that a centralized team of dedicated vulnerability management professionals will be more effective and efficient for our future operations. This will allow for more consolidated training to a smaller subset of staff, rather than training multiple persons across 70+ agencies. Furthermore, having one manager oversee this centralized team will allow for more consistent training plans and oversight of individual needs.

Executive management of MN.IT Services is ultimately accountable for the audit finding resolutions. Our manager over vulnerability management, working in conjunction with our agency training coordinator, will be responsible for implementing changes to our training materials. Resolution tactics, with anticipated milestone dates, will be included in our information security two-year tactical plan, due to be completed by July 1, 2012. Mark Mathison, our Information Security Manager over Governance, Risk and Compliance will oversee resolution efforts. We anticipate resolution to be completed by December 31, 2012.

Once again, I would like to thank you and your staff for the outstanding effort on this audit.

Sincerely,

Carolyn Parnell
State Chief Information Officer