OLA

OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA

Financial-Related Audit

Public Employees Retirement Association

Computer System Security Audit

SEPTEMBER 19, 2002 **02-62**

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 fifty 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 and one best practices review.

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 651-296-1727 (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, evaluation, or best practices review, please contact us at 651-296-4708 or by e-mail at auditor@state.mn.us

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

Senator Ann. H. Rest, Chair
Legislative Audit Commission

Members of the Legislative Audit Commission

Ms. Mary Most Vanek, Executive Director
Public Employees Retirement Association

We have conducted an information technology audit of select activities at the Public Employees Retirement Association. Our audit scope assessed the adequacy of computer security controls. The individual chapters of this report discuss the specific audit objectives and conclusions that we reached.

We conducted our audit in accordance with *Government Auditing Standards*, as issued by the Comptroller General of the United States. These 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 Public Employees Retirement Association complied with the provisions of laws, regulations, contracts, and grants significant to the audit. The association's management is responsible for establishing and maintaining the internal control structure and for compliance with applicable laws, regulations, contracts, and grants.

This report is intended for the information of the Legislative Audit Commission and the management of the Public Employees Retirement Association. This restriction is not intended to limit the distribution of this report, which was released as a public document on September 19, 2002.

/s/ James R. Nobles

James R. Nobles
Legislative Auditor

/s/ Claudia J. Gudvangen

Claudia J. Gudvangen, CPA
Deputy Legislative Auditor

End of Fieldwork: May 31, 2002

Report Signed On: September 16, 2002

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

Public Employees Retirement Association
Computer System Security Audit

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	Audit Manager
Eric Wion, CPA, CISA	Auditor-In-Charge
Scott Tjomsland, CPA	Auditor

Exit Conference

We discussed the findings and recommendations with the following representatives of the Public Employees Retirement Association at the exit conference held on September 9, 2002.

Mary Most Vanek	Executive Director
David DeJonge	Chief Information and Financial Officer
Richard Rademaker	Computer Operations Supervisor

Public Employees Retirement Association
Computer System Security Audit

Report Summary

"Security weaknesses exposed PERA's critical business data to extreme risk from both inside and outside the organization."

Conclusions:

The Public Employees Retirement Association (PERA) does not have a comprehensive security program that is capable of responding promptly to volatile technology risks. Of greatest concern, the retirement association had not devoted sufficient staff to perform important security duties. At the time of our audit, one information technology professional managed most aspects of the security infrastructure. No backup employees had been cross-trained to perform these critical security duties. Compounding this risk, PERA had not completed a formal information technology risk assessment or developed written security policies, procedures, and standards. Finally, the retirement association had very few monitoring controls to detect and promptly respond to potential security breaches.

These security program shortcomings allowed serious internal control weaknesses to go unchallenged:

- PERA did not protect its computer infrastructure from some Internet-based attacks.
- Software running on some servers had not been updated to remedy known security flaws.
- PERA did not properly secure its databases.
- PERA did not adequately secure some data on its servers or enforce strong password controls.
- PERA did not limit the number of network access points.

Financial-Related Audit Reports address internal control weaknesses and noncompliance issues found during our audits of state departments and agencies. The scope of our work at the Public Employees Retirement Association was limited to a review of controls that protect the integrity of its mission critical business data.

This page intentionally left blank.

Chapter 1. Introduction

This information technology audit assessed the adequacy of computer security controls at the Public Employees Retirement Association (PERA) as of May 2002. PERA developed a complex computer infrastructure to administer its four pension funds:

- Public Employees Retirement Fund
- Public Employees Police and Fire Fund
- Public Employees Correctional Fund
- Public Employees Defined Contribution Plan

Approximately 3,500 counties, cities, townships, school districts, and other local units of government contribute to PERA's four pension funds. Collectively, these four funds hold retirement assets for nearly 318,000 active and former employees and their beneficiaries. At June 30, 2001, the retirement association reported that its pension funds had $14.2 billion in net assets. Fiscal year 2001 retirement contributions and payments to beneficiaries were $461.1 and $807.8 million, respectively.

PERA's computer infrastructure includes an array of powerful computers that are commonly referred to as "servers." These servers house many mission critical business systems that the retirement association uses to record employer contributions, pay beneficiaries, maintain beneficiary demographic data, and prepare required financial reports. These servers also house a series of large databases that contain most of PERA's critical business data.

PERA deployed four layers of security to protect its mission critical business systems and data. The first layer of security, called a firewall, helps shield the computer infrastructure from unscrupulous people on the Internet. The second layer of security, embedded in each business system, restricts employees to specific computer screens that they must use to fulfill their job duties. Customizable security features in the databases provide the third layer of security. When properly configured, these features prevent people from directly connecting to the database to modify data. Finally, the servers used by PERA have many customizable security features that can be used to restrict access to sensitive computer programs and data. The servers also use unique logon ID codes and passwords to validate the identity of people.

Chapter 2 discusses the scope, objectives, and methodology that we used to conduct this information technology audit. Chapter 2 also discusses the conclusions that we reached and offers recommendations to improve the security infrastructure.

This page intentionally left blank.

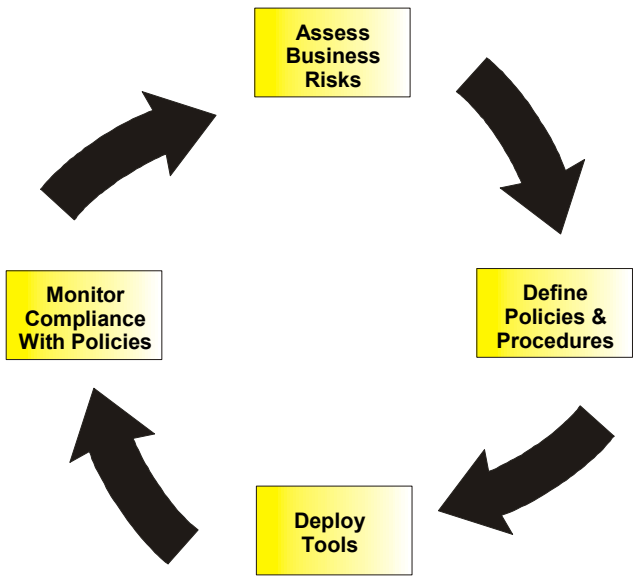
Chapter 2. Computerized Access Controls

Chapter Conclusions

Security weaknesses exposed PERA's critical business data to extreme risk from both inside and outside the organization. Our audit identified firewall configuration weaknesses that could have let unauthorized people gain access to the retirement association's computer network. We also found significant weaknesses in database and server security controls. The management of PERA must address these security weaknesses immediately to prevent a disastrous loss or the unauthorized disclosure of confidential information.

With the rapid proliferation of the Internet, 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, much like buying insurance. 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 were sanctioned by management. Information provided by these tools helps organizations monitor compliance with their policies and procedures and fine-tune subsequent risk assessments in the ongoing security management lifecycle.

Figure 2-1
The Ongoing Security Management Lifecycle



Source: Auditor Prepared

Audit Objective and Methodology

This information technology audit assessed the adequacy of computer security controls at PERA. Specifically, we designed our work to answer the following question:

- Did PERA design and implement adequate controls to protect the integrity of its mission critical business data?

To answer this question, we interviewed and obtained documentation from information technology professionals. We also used a variety of different computer-assisted auditing tools to analyze the security infrastructure, including servers, personal computers, database management systems, and the firewall. We did not, however, review security controls that are embedded in the retirement association's business systems. Those controls are considered each year as part of PERA's annual financial statement audit.

Evaluation Criteria

We obtained our evaluation criteria from the Control Objectives for Information and Related Technology (COBIT), published by the Information Systems Audit and Control Foundation. The mission of COBIT is:

> *To research, develop, publicize and promote an authoritative, up-to-date, international set of generally accepted information technology control objectives for day-to-day use by business managers and auditors.*

The COBIT Framework includes 34 high-level control objectives and 318 detailed control objectives, grouped in the following four domains:

Planning and Organization	This domain covers strategic planning and concerns the ways that information technology can best contribute to the achievement of business objectives. It addresses the need to plan, communicate, and manage a strategic vision.
Acquisition and Implementation	This domain includes control objectives that pertain to acquiring, developing, and implementing information technology solutions. It also covers control objectives that pertain to changing existing systems.
Delivery and Support	This domain includes the processes that must be in place to deliver information technology services on a daily basis. Some of these processes include ensuring systems security and managing data.
Monitoring	This domain addresses the need to regularly assess the quality of information technology processes. It addresses management's oversight of the control processes and independent assurance provided by internal and external audit.

Conclusions

PERA deployed a variety of different security tools. However, these tools were not part of a comprehensive and ongoing security management program. As discussed in Finding 1, the retirement system had not undergone a formal information technology risk assessment or fully documented its security policies, procedures, and standards. Furthermore, it had not developed sufficient procedures to monitor and periodically reassess the adequacy of its security controls. Finally, we question whether PERA devoted sufficient staff to perform important security duties.

This audit uncovered many security weaknesses that exposed the retirement association's critical business data to significant risk**.** In Finding 2, we discuss configuration problems that limited the effectiveness of the retirement association's firewall. Finding 3 discusses security weaknesses that resulted from not promptly installing patches to commercial software products. In Finding 4, we discuss an assortment of different security weaknesses in PERA's databases. Finding 5 discusses security weaknesses that resulted from granting accounts excessive access, not properly securing critical directories and files, and not enforcing strong password controls. Finally, Finding 6 discusses security weaknesses that resulted from not limiting the number of network access points.

Current Findings and Recommendations

1. PERA did not design and implement an effective security program.

PERA does not have a comprehensive security program that is capable of responding promptly to volatile technology risks. Of greatest concern, the retirement association had not devoted sufficient staff to perform important security duties. At the time of our audit, one information technology professional managed most aspects of the security infrastructure. No backup employees had been cross-trained to perform these critical security duties. Compounding this risk, PERA had not completed a formal information technology risk assessment or developed written security policies, procedures, and standards. Finally, the retirement association had very few monitoring controls in place to detect and promptly respond to potential security breaches.

The resulting security infrastructure that we examined was a patchwork of automated tools that lacked a cohesive policy foundation. As illustrated in Figure 2-1, security controls need to be the product of an ongoing risk management process. There are many information technology risk assessment tools and methodologies. However, most 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 standards that are commensurate with risk. It is important to document this information because it provides security professionals with criteria to configure security tools and make consistent access control decisions. Documentation also helps ensure the continued understanding and operation of critical security controls, should key employees leave the organization.

Unfortunately, history has shown that it is virtually impossible to design a flawless security infrastructure. This inherent security administration problem is why every organization must vigilantly monitor its systems for signs of attack. PERA configured some of its commercial software products to log selected security events. However, many critical events, including firewall activities, were not logged or monitored. Furthermore, PERA had not deployed any intrusion detection software to streamline monitoring duties. When unusual events occur, intrusion detection software packages can immediately contact the appropriate individual to begin an investigation.

Finally, PERA had not tested its security infrastructure with vulnerability assessment tools to search for commonly know security weaknesses. Vulnerability scanners are special software packages that probe systems to find security weaknesses. An example of one such weakness is a bug in a commercial software product that could allow a hacker to gain control of a computer system. Vendors that provide 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. In our audits, we use a vulnerability assessment tool that found many of the security weaknesses cited in this report.

Recommendations

- *PERA should perform periodic information technology risk assessments and use the data to develop written security policies, procedures, and standards.*
- *PERA should allocate additional staff to perform security duties.*
- *PERA should develop procedures to monitor its security infrastructure for signs of attack and periodically scan the infrastructure for common security vulnerabilities.*

2. PERA did not protect its computer infrastructure from some Internet-based attacks.

Firewall configuration weaknesses could have let unscrupulous individuals on the Internet gain unauthorized access to PERA's computer network. A firewall is a computer that separates an organization's private network from the public Internet. Serving as 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 in firewall rules, is not allowed to pass.

While examining firewall rules, we found several types of Internet traffic that were not appropriately filtered. These types of configuration weaknesses are significant because hackers on the Internet can detect them quite easily with automated tools. Furthermore, once inside the firewall, every computer, database, and network component becomes a potential target of attack.

Recommendation

- *To the extent possible, PERA should modify its firewall rules to restrict incoming Internet traffic.*

3. Software running on some servers had not been updated to remedy known security flaws.

PERA did not promptly install security-related software patches on some of its servers. The retirement association uses many commercial software packages. Unfortunately, computer hackers routinely discover and exploit flaws in commercial software to gain unauthorized access to 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.

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. Also, organizations need formal testing and installation procedures that include an exit strategy, should a software patch result in a system failure.

Recommendation

- *PERA should develop procedures to promptly test and install security-related software patches.*

4. PERA did not properly secure its databases.

Numerous database security weaknesses exposed critical business data to an unacceptably high risk of loss or unauthorized disclosure. Of greatest significance, some accounts were not password protected. Some of these unprotected accounts could perform database administration duties. Securing database administration accounts is critical because they have complete and unfettered access to all data. Recognizing this capability, computer hackers often use automated tools to find and exploit database accounts that have not been properly secured.

PERA also did not develop controls to prohibit employees from directly connecting to its databases from outside the intended business systems. Typically, all changes to data should be made through business systems. Data changes that are not made through business systems are risky because they circumvent important data integrity edits. Furthermore, employees who are unfamiliar with technical database design details could make changes that render the database useless. Given these significant risks, organizations should limit direct database connectivity to select employees who perform database maintenance or have other justifiable business needs.

When possible, employees who need direct connectivity should be granted "read-only" clearance.

We also found some sample databases and powerful database management programs that had not been removed. Commercial software vendors typically offer many components and features that organizations do not need to conduct business. It is important to remove these components, when possible, because they often contain bugs that can be compromised by hackers. Since some unused components cannot be removed, it is also important to promptly install all security-related software patches.

Finally, we found several information technology staff that had excessive security clearances that were not necessary. Granting staff excessive access exposes data to an unnecessary risk of loss.

Recommendations

- *PERA should password protect all accounts that can access its databases.*
- *PERA should prohibit employees from directly connecting to databases unless there is a justifiable business need.*
- *PERA should remove unnecessary software components from its database environments.*
- *PERA should limit staff to the minimum security clearances necessary.*

5. PERA did not adequately secure some data on its servers or enforce strong password controls.

Many accounts used by employees and installed software products had powerful security clearances that were not necessary. We found many critical directories and files that could be modified or deleted by inappropriate people. Some of these directories and files were essential parts of the computer operating system, while others contained sensitive business data. We also found installed software accounts that had unnecessarily high security clearances. Granting accounts excessive security clearances exposes data to an unnecessary risk of loss.

PERA also did not enforce strong password management controls. For example, one policy required employees to share their passwords with the information technology unit, who then stored the passwords in an electronic file. Sharing passwords is unacceptable because it reduces individual accountability. Once a password has been shared, it is virtually impossible to prove that a given individual initiated a specific computerized transaction. Finally, PERA did not configure its security controls to force users to select strong passwords. Strong passwords are those that are difficult for hackers to guess with automated tools.

Recommendations

- *PERA should limit personal and software accounts to the minimum security clearances necessary.*

- *PERA should prohibit password sharing.*

- *PERA should force employees to select strong passwords.*

6. PERA did not limit the number of access points into its private network.

PERA installed software on most of its computers that allowed people to connect to and operate their computers from remote locations, such as their homes. Providing numerous network access points makes it difficult to effectively 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, firewall rules must be written less restrictively to allow Internet traffic to reach many different locations in the private network. Configuration errors on any of these computers that are accessible from the Internet could expose all data and computers in the private network to significant risk.

Recommendation

- *PERA should limit the number of access points into its network.*

This page intentionally left blank.

Public Employees
Retirement Association
of Minnesota

September 13, 2002

James R. Nobles, Legislative Auditor
Office of the Legislative Auditor
Centennial Office Building
658 Cedar Street
St. Paul, MN 55155

Dear Mr. Nobles:

The following information is offered in response to your draft audit report dated August 29, 2002. PERA is committed to providing a secure environment for the data we receive and retain in our databases. We have several checks and reconciliation reports we constantly run to check the accuracy of our data and are quite confident that, though your office concluded our databases could potentially be "hacked," the integrity of our data has not been jeopardized. We take our responsibility to secure data and applications very seriously and have made several changes to tighten that security. We will continue to work toward improvements in the future.

Recommendation
PERA should perform periodic information technology risk assessments and use the data to develop written security policies, procedures, and standards.

Response
We agree that we do not have formal written security policies, procedures and standards in place. We do have ongoing information technology risk assessments on a regular basis, but generally have not had the time or personnel it takes to write down the results in a formal document. We are in the process of hiring a second network administrator who will be asked to help with this process. We will begin to develop more formal risk assessments and document the resulting security policies, procedures, and standards. We will also assess the effectiveness of handling such a program internally and determine if we need to contract with outside vendors to help us through that process. Should we need additional contracted help to develop a formal program, we will attempt to get additional funding during the next budget process.

Person Responsible: Dave DeJonge

Estimated Completion Date: July 2003

Recommendation
PERA should allocate additional staff to perform security duties.

Response
We agree and have tried for the past 5 years to hire and retain additional help. We lost two support personnel last year to better paying jobs in the private sector. We were in the process of writing an updated PD for a full-time network/security administrator when the audit began. We are still in the process of hiring, and hope to have a full-time employee on board by October.

Person responsible: Dave DeJonge

Estimated completion date: October 2002

Recommendation
PERA should develop procedures to monitor its security infrastructure for signs of attack and periodically scan the infrastructure for common security vulnerabilities.

Response
We agree and have already begun monitoring our security infrastructure for signs of attack. We are in the process of formalizing procedures for how we handle the information received via the monitoring software. We have sent an employee to an extensive course on hacking methods so that we are more aware of where we might be vulnerable from attacks. We are also reviewing new tools that might be used to monitor our infrastructure. On an on-going basis we will continue to assess our situation and determine if we need additional monitoring tools or better ways to deal with the data we receive. We will also periodically scan the infrastructure for common security vulnerabilities.

Person responsible: Dave DeJonge

Estimated completion date: December 2002

Recommendation
To the extent possible, PERA should modify its firewall rules to restrict incoming Internet traffic.

Response
We have always restricted incoming Internet traffic via a firewall. The specific instances cited by the auditor have been addressed. We will continue to review and assess our firewall rules on a regular basis.

Person responsible: Dave DeJonge

Estimated completion date: Completed

Recommendation

PERA should promptly install security-related software patches.

Response

We agree that keeping software up to date is critical to enforce proper security, and are in the process of updating our systems with the most current hotfixes, service packs and security updates. This process is not foolproof and may introduce unintended or unexpected results on key production systems. Therefore, we are being extremely cautious when dealing with servers providing critical organizational operations. We are making a concerted effort toward applying all relevant updates to all systems, and intend to stay up to date with future updates. PERA is utilizing several tools to assist in identification, review and installation of the appropriate updates. We will be developing formal processes to identify and review new patches, determine the necessity and risks associated with the patch, which equipment is affected by the patch, and how quickly it needs to be applied.

Person responsible: Dave DeJonge

Estimated completion date: December 2002

Recommendation

PERA should password protect all accounts that can access its databases.

Response

We agree and are in the process of password protecting those accounts and testing the changes to make sure our software still works correctly. We have found that the functionality of some applications has been adversely affected by retroactively applying passwords. We are reviewing those situations in order to determine and implement a secure solution that does not restrict functionality. Database accounts will be reviewed periodically, eliminating unused accounts and to determine the validity of access for individual users.

Person responsible: Dave DeJonge

Estimated completion date: April 2003

Recommendation

PERA should prohibit employees from directly connecting to databases unless there is a justifiable business need.

Response

We agree and were in the process of doing that when the audit began. We are doing two things to fix this problem. First, we are building a database that replicates our production database so that those employees who need information directly from the database can get that information without actually connecting to our production database. Second, we are changing the security on our production database to application level security. We are in the process of implementing both of those.

Person Responsible: Dave DeJonge

Estimated completion date: March 2003

Recommendation
PERA should remove unnecessary software components from its database environment.

Response
We agree and our DBA and Network Administrator are looking for unnecessary software components and deleting them from our system.

Person Responsible: Dave DeJonge

Estimated completion date: March 2003

Recommendation
PERA should limit staff to the minimum security clearances necessary.

Response
We agree and are reviewing our security to make sure we grant security appropriately. Since the audit's fieldwork was completed, security clearances have been reassessed for the users identified in the audit. If access rights are not needed, we are removing them on an on-going basis. As stated earlier, we are in the process of replicating our database and giving employees access to the copied database instead of the production database. When the replicated database is available we will re-analyze security clearances for those individuals and adjust them accordingly.

Person Responsible: Dave DeJonge

Estimated completion date: April 2003

Recommendation
PERA should limit personal and software accounts to the minimum security clearances necessary.

Response
We agree and assessed our directory structure and the rights assigned to personnel and software accounts. The vast majority of our personal accounts already had minimum security clearances since we look at those accounts on an annual basis. We are in the process of changing the way some of our software accounts interact with other software, databases and servers to see if there are ways we can reduce security clearances on our software accounts.

Person Responsible: Dave DeJonge

Estimated completion date: May 2003

Recommendation
PERA should prohibit password sharing.

Response
We do not agree with this finding. Employees presently share their login password with our network administrator and help desk administrator, and only those two people. Those two individuals assist users when they have computer problems and handle all of our upgrades and maintenance issues. They need to ensure that software is properly configured and works properly for the specific user of each machine. Since all machines are password protected, the two administrators either need to know the users' password or reset the users' password in order to access the system. We analyzed the risks and benefits associated with both methods, and determined that, for us at this time, it is riskier to allow administrators to reset passwords.

We believe our method has less risk and has the additional benefit of allowing administrators to provide help to our users in setting passwords. We find that many of our users struggle when trying to develop proper passwords, and our administrators often need to help them develop stronger passwords.

We are presently upgrading much of our software, and our administrators are spending a lot of time working on individual PCs configuring the new software for specific users. Once our systems are upgraded and working in the new environment we will take another look at this issue and make another assessment of whether or not our method of security warrants a change.

Recommendation
PERA should force employees to select strong passwords.

Response
We enforced strong passwords before, during and after the audit, though not directly through software. Since each password is reviewed by an administrator, we manually force employees to select strong passwords. If an employee changes a password to a password that isn't considered "strong," the administrator forces them to change it to a strong password. Though we have reviewed various alternatives for forcing strong passwords automatically, we have not found a solution that works well in our present configuration. We will continue to analyze our alternatives and hope to find a solution that works with our systems.

Person Responsible: Dave DeJonge

Estimated completion date: Completed

Recommendation
PERA should limit the number of access points into its network.

Response
We agree and limited the number of access points through our firewall immediately once the auditors pointed out this weakness. We will continue to review and monitor our access points on an on-going basis.

Person Responsible: Dave DeJonge

Estimated completion date: Completed

Sincerely,

/s/ Mary Most Vanek

Mary Most Vanek
Executive Director