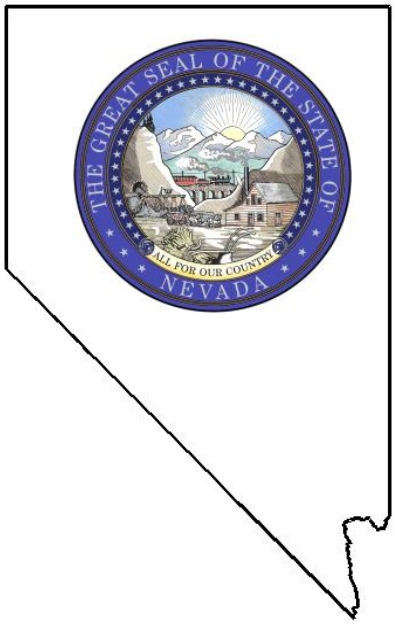
LA16-15

STATE OF NEVADA

Performance Audit

Department of Administration
Division of Human Resource Management
Information Security

2016



Legislative Auditor
Carson City, Nevada

Audit Highlights

Highlights of performance audit report on the Department of Administration's Division of Human Resource Management, Information Security issued on October 18, 2016. Legislative Auditor report # LA16-15.

Background

The Division of Human Resource Management is within the Department of Administration. The mission of the Division is to provide exceptional human resource services with integrity, respect, and accountability. The Division is divided into seven sections which provide services to state employees, state agencies, and the general public.

The Division has two offices, one in Carson City and the other in Las Vegas.

The state Department of Personnel became the Division of Human Resource Management, within the Department of Administration, during a State government reorganization that became effective in July of 2011. The Division was authorized 75 full-time equivalent employees and had expenditures of $7.9 million in fiscal year 2015.

The Division has no information technology staff of its own. The Division relies on the Division of Enterprise Information Technology Services for all of its information technology support.

Purpose of Audit

The purpose of our audit was to determine if the Division of Human Resource Management has adequate information security controls in place to protect the confidentiality, integrity, and availability of its information and information processing systems. Our audit covered the systems and practices in place from March to August of 2015.

Audit Recommendations

This audit report contains 11 recommendations to improve the security over the Division's information systems. The Division of Human Resource Management accepted the 11 recommendations.

Recommendation Status

The Division of Human Resource Management's 60-day plan for corrective action is due on January 19, 2017. In addition, the six-month report on the status of audit recommendations is due on July 19, 2017.

Division of Human Resource Management, Information Security

Department of Administration

Summary

Confidential information about state employees was stored unencrypted in the Division's databases, increasing the risk of unauthorized access of this information. State security standards require that confidential personal data be encrypted whenever possible. In addition, weaknesses exist in managing network users. These weaknesses include not disabling former employee computer accounts when they leave Division employment and some staff had not completed their annual information technology security awareness training.

Desktop computers used by Division employees lacked adequate virus protection and were missing Windows operating system security updates. In addition, some of the Division's servers lacked adequate virus protection and contained security vulnerabilities due to missing operating system updates. These deficiencies make computers more vulnerable.

Controls were not in place to ensure sensitive information stored in the Division's photocopiers was erased. Office copiers contain hard drives that store information. This data must be deleted prior to the photocopiers being replaced or there is a risk that the sensitive information could remain on the copiers' hard drives when they leave Division control.

Key Findings

Confidential information about state employees was stored unencrypted in the Division's databases, increasing the risk of unauthorized access of this information. One database contained Social Security numbers of over 145,000 current and former state employees and their beneficiaries. State security standards require that confidential personal data be encrypted whenever possible. However, this confidential personal information was not encrypted in the Division's databases. Enterprise Information Technology Services (EITS) support staff, who manage the Division's databases, indicated they were not aware that there was a requirement to encrypt this information. (page 3)

Weaknesses exist in managing network users. We identified 42 computer accounts of former staff among the 179 Division computer user accounts whose network credentials (login identification and passwords) had not been disabled. Thirty-one of these former employees had been gone for over one year. One employee had been gone almost 10 years. Untimely disabling of former employees' network credentials increases the risk that someone could gain unauthorized access to the state's information and systems. (page 4)

Five of the Division's 77 staff had not completed their annual security awareness training. State security standards require that state employees each receive annual information technology security awareness refresher training to ensure they stay aware of current security threats as well as understanding their responsibility to keep state information confidential. (page 5)

Desktop computers lacked adequate virus protection. Seven of the Division's 85 computers did not have adequate virus protection installed. State security standards require that virus protection software be updated regularly to retain protection from evolving online threats. Without current virus protection installed, computers could become infected with malicious software. (page 6)

Seventeen of the Division's 85 computers were not receiving Windows operating system updates on a regular basis. Operating system updates are released monthly by Microsoft. State security standards require updates be installed timely to fix security vulnerabilities. Computers without current software security patches installed represent weaknesses in a computer network that can be exploited by a malicious entity to gain unauthorized access to state computer resources and sensitive data stored on them. (page 6)

Some servers had vulnerabilities. For example, one of the Division's four servers did not have virus protection software installed. Without current virus protection software installed, servers could become infected with malicious software. In addition, three of the four servers had critical or high-level vulnerabilities due to missing Windows operating system updates. Without installation of these software patches, computers remain vulnerable to online threats. (page 8)

The Division's office copiers were not configured to securely process confidential information. Four of the Division's six photocopiers did not have the Immediate Image Overwrite function enabled as required by state security standards. This function configures the device to erase the processed job immediately after the copy, scan, or fax job is completed, thereby reducing the likelihood of any confidential information being stored on the copier's hard drive. (page 10)

STATE OF NEVADA
LEGISLATIVE COUNSEL BUREAU
LEGISLATIVE BUILDING
401 S. CARSON STREET
CARSON CITY, NEVADA 89701-4747

LEGISLATIVE COMMISSION (775) 684-6800
MICHAEL ROBERSON, *Senator, Chairman*
Rick Combs, *Director, Secretary*

INTERIM FINANCE COMMITTEE (775) 684-6821
PAUL ANDERSON, *Assemblyman, Chairman*
Cindy Jones, *Fiscal Analyst*
Mark Krmpotic, *Fiscal Analyst*

RICK COMBS, *Director*
(775) 684-6800

BRENDA J. ERDOES, *Legislative Counsel* (775) 684-6830
ROCKY COOPER, *Legislative Auditor* (775) 684-6815
SUSAN E. SCHOLLEY, *Research Director* (775) 684-6825

Legislative Commission
Legislative Building
Carson City, Nevada

This report contains the findings, conclusions, and recommendations from our performance audit of the Department of Administration, Division of Human Resource Management, Information Security. This audit was conducted pursuant to the ongoing program of the Legislative Auditor as authorized by the Legislative Commission. The purpose of legislative audits is to improve state government by providing the Legislature, state officials, and Nevada citizens with independent and reliable information about the operations of state agencies, programs, activities, and functions.

This report includes 11 recommendations to improve security over the Division's information systems. We are available to discuss these recommendations or any other items in the report with any legislative committees, individual legislators, or other state officials.

Respectfully submitted,

Rocky Cooper, CPA
Legislative Auditor

August 9, 2016
Carson City, Nevada

Division of Human Resource Management
Information Security
Table of Contents

Introduction

Background

The Division of Human Resource Management (Division) is within the Department of Administration. The mission of the Division is to provide exceptional human resource services with integrity, respect, and accountability. The Division is divided into seven sections which provide services to state employees, state agencies, and the general public. The seven sections include:

- Agency Human Resource Services
- Central Payroll
- Central Records
- Compensation, Classification, and Recruitment Section
- Consultation and Accountability
- EEO and Discrimination Investigation Unit
- Office of Employee Development

The Division has two offices, one in Carson City and the other in Las Vegas.

The State Department of Personnel became the Division of Human Resource Management, within the Department of Administration, during a state government reorganization that became effective in July of 2011. The Division was authorized 75 full-time equivalent employees and had expenditures of $7.9 million in fiscal year 2015.

The Division has no information technology (IT) staff of its own. The Division relies on the Enterprise Information Technology Services (EITS) for all of its IT support.

Scope and Objective

The scope of our audit was the systems and practices in place from March to August of 2015. Our audit objective was to:

- Determine whether the Division of Human Resource Management has adequate information security controls in place to protect the confidentiality, integrity, and availability of its information and information processing systems.

This audit is part of the ongoing program of the Legislative Auditor as authorized by the Legislative Commission, and was made pursuant to the provisions of NRS 218G.010 to 218G.350. The Legislative Auditor conducts audits as part of the Legislature's oversight responsibility for public programs. The purpose of legislative audits is to improve state government by providing the Legislature, state officials, and Nevada citizens with independent and reliable information about the operations of state agencies, programs, activities, and functions.

Confidential Information About State Employees Needs Better Protection

Confidential information about state employees was stored unencrypted in the Division's databases, increasing the risk of unauthorized access to this information. The Division collects sensitive information of state employees that is considered confidential. For example, one database contained Social Security numbers of over 145,000 current and former state employees and their beneficiaries. State security standards require that confidential personal data be encrypted whenever possible. However, this confidential personal information was not encrypted in the Division's databases. EITS support staff, who manage the Division's databases, indicated they were not aware that there was a requirement to encrypt this information.

Encrypting the data would better protect this sensitive information should a malicious person gain unauthorized access to these databases. Unauthorized access of this sensitive information could result in identity theft-related problems for employees whose personal data is compromised. In addition, the Division would be required to notify all the impacted employees of the information release as well as various credit monitoring agencies, a potentially time consuming and expensive task. Furthermore, the public could lose faith in the state's ability to protect the personal information that the State requires the public to provide for various services and licensing requirements.

Recommendation

1. Encrypt confidential personal data in Division databases at the earliest opportunity.

Weaknesses Exist in Managing Network Users

Weaknesses exist in managing the Division's network users. These weaknesses include not disabling former employee computer accounts when they leave Division employment. In addition, some employees had not conducted their annual information technology security awareness training.

Former Staff Had Current Network Access

Former employees' computer accounts were not disabled when they left the Division. We identified 42 computer accounts of former staff among the 179 Division computer user accounts we examined whose network credentials (login identification and passwords) had not been disabled. Thirty-one of these former employees had been gone for over 1 year. One employee had been gone almost 10 years. Security standards require employee computer accounts be disabled timely upon an employee's departure to reduce the risks of possible unauthorized access of the state's data or systems.

The Division's procedure for disabling computer accounts of terminating or transferring employees was not effective. The procedure utilized a Termination/Transfer Checklist that served as a supervisory reminder of steps to complete when an employee leaves the Division. However, according to Division management, there was no requirement to document completion of any of these steps on the checklist nor did any other Division employee verify their completion. In addition, when the EITS Help Desk was informed of an employee's departure, there was no requirement to follow up and verify the departing employee's computer accounts were disabled. Untimely disabling of former employees' network credentials (logins and passwords) increases the risk that someone could gain unauthorized access to the state's information and systems.

Some Staff Did Not Complete Annual Security Awareness Training

Five of the Division's 77 staff had not completed their annual security awareness training. State security standards require that state employees each receive annual IT security awareness refresher training to ensure they stay aware of current security threats as well as understanding their responsibility to keep state information confidential. Without completing such training, there is greater risk that employees will not properly protect the information and information systems they use.

This situation arose as a result of several employees not heeding the periodic reminders sent by the Division's information security officer to complete their training. The five employees completed their annual security awareness training after the omission was brought to the Division's attention during the audit.

Recommendations

2. Implement a more effective procedure to ensure departing employees' computer accounts are disabled timely.
3. Implement quarterly reviews of computer user accounts, as required by state security standards, to identify any former staff whose computer accounts were not disabled when they terminated employment with the Division.
4. Periodically reemphasize the Division's commitment to seeing that all employees complete their annual security awareness training.

Desktop Computers Had Inadequate Security

Desktop computers used by Division employees lacked adequate virus protection and were missing Windows operating system security updates. These two deficiencies make these computers more vulnerable to online threats.

Some Desktop Computers Lacked Adequate Virus Protection

Some of the Division's 85 computers were lacking current virus protection. Specifically, 7 of the 85 computers, or 8%, did not have adequate virus protection installed. State security standards require that virus protection software be updated regularly to retain protection from evolving online threats. EITS staff indicated this problem was the result of incomplete antivirus software installations.

Without current virus protection software installed, computers could become infected with malicious software attached to infected emails or from infected websites. Employees whose computers do become infected will lose productive time until the malware is removed from their computers. In addition, some malware that infects computers is capable of gaining access to sensitive information that resides on the infected computer or elsewhere on the network.

Desktop Computers Were Missing Windows Operating System Updates

Numerous computers showed gaps in the installation of operating system updates. Seventeen of the 85 computers, or 20%, were not receiving Windows operating system updates on a regular basis.

Operating system updates are released monthly by Microsoft. State security standards require these updates be installed timely in order to fix security vulnerabilities that have been identified in the Windows operating system software. EITS staff indicated that a technical issue caused some computer operating system software updates to fail. Computers without current software

security patches installed represent weaknesses in a computer network that can be exploited by a malicious entity to gain unauthorized access to state computer resources and sensitive data stored on them.

In addition, 5 of these 17 exceptions were laptop computers. Division staff indicated there is not currently any requirement or procedure to periodically update laptop operating systems nor the virus protection software on these computers.

Recommendations

5. Implement a procedure to periodically review the status of all Division computers to identify computers without up-to-date virus protection.
6. Implement a procedure to periodically check Windows operating system software update installations to detect failed or missing updates.
7. Develop a Division policy and procedure requiring employees with laptop computers to periodically update the virus definitions and install Windows operating system updates timely.

Some Servers Had Vulnerabilities

Some of the Division's four servers lacked adequate virus protection. Other servers contained security vulnerabilities due to missing operating system updates. Both conditions increase the risk that these servers could be infected with a virus and become vulnerable to attacks.

Server Lacked Virus Protection Software

One of the four servers did not have Symantec Endpoint Protection (virus protection software) installed. State security standards require servers have current virus protection software installed. Without current virus protection software installed, servers could become infected with malicious software. Servers represent a computing resource that is shared by the entire Division. When a server becomes infected with malware, or otherwise compromised, the productivity of the entire Division could be affected and the security of the information on the server could be compromised.

Servers Had High Level Vulnerabilities

Three of the four servers had critical or high-level vulnerabilities due to missing Windows operating system updates. State security standards require these updates be installed timely to fix security vulnerabilities that have been identified in the Windows operating system software. Without installation of these software patches, computers remain vulnerable to online threats.

Both of the above conditions were the result of not having service agreements between the Division and EITS that specified that EITS should provide these services to the Division's servers. The Division indicated this omission of service agreements was an unintentional consequence of the state's 2011 reorganization that made the Department of Personnel a Division within the Department of Administration. That reorganization resulted in the Division losing its IT support staff who were reassigned to EITS.

As a result, the Division had no IT support staff of its own to continue maintaining these servers.

Recommendations

8. Establish a procedure with EITS that includes providing the Division with documentation to independently verify that servers have current virus protection as well as Windows operating system updates installed.
9. Ensure all Division servers maintained by EITS have current service agreements.

Photocopiers Were Not Securely Configured

Controls were not in place to ensure sensitive information stored in the Division's six photocopiers was erased. Office copiers contain hard drives that store information. This information is stored when employees make copies, fax, scan, or print documents on these machines. This information is stored inside the photocopiers on internal hard drives, which are the same storage devices as contained in desktop computers. This data must be deleted prior to the photocopiers being replaced or there is a risk that the sensitive information could remain on the copiers' hard drives when they leave Division control.

The Division's office copiers were not configured to securely process confidential information. Four of the six photocopiers tested did not have the Immediate Image Overwrite function enabled as required by state security standards. This function configures the device to erase the processed job immediately after the copy, scan, or fax job is completed, thereby reducing the likelihood of any confidential information being stored on the copier's hard drive. Division staff sometimes process confidential personal information on these copiers.

Division staff indicated they were not aware that office copiers contained hard drives that could store the confidential information processed on these devices. Nor were staff aware of the need to remove the data from the copiers before the copiers left Division and state control. State security standards require these devices be configured with the Immediate Image Overwrite function enabled. In addition, security standards also require the hard drives be removed or securely erased before the copiers leave state control.

Recommendations

10. Train staff to be aware that office copiers contain hard drives that store processed information and this information should be erased when each copier is replaced.
11. Implement procedures to ensure that photocopiers are configured to not store processed data as indicated in state security standards.

Appendix A
Audit Methodology

To gain an understanding of the Division of Human Resource Management, we interviewed Division management and staff. We interviewed the Division's EITS support staff to gain a broad understanding of the Division's information technology resources and how they are organized, managed, and utilized. Further, we documented and assessed the internal controls over information technology systems, users, and data resources.

To determine if controls over desktop computer security were adequate, we examined the entire population of computers in current use by Division personnel. We tested a combined total of 85 computers being used in the Carson City and Las Vegas offices. We tested these computers to ensure they had current virus protection as well as the latest operating system security updates.

We examined the Division's population of 179 network user accounts to determine if only current employees had access to the network. In addition, we determined if all currently assigned Division employees had conducted their annual information technology security awareness training. Furthermore, we determined if the Division was conducting background investigations on its employees who had access to confidential information.

We examined the security of the Division's two telecommunications rooms to ensure the equipment contained in them was adequately secured. To assess the security of the Division's two network servers, we tested to ensure they were configured to enforce state password standards for all accounts, were protected with virus protection software, and had appropriate operating system software updates installed timely. We verified that any wireless networks used by the Division were authorized and had proper

security controls in place. We reviewed the security of confidential personal data used and stored by the Division to ensure it was adequately protected. We reviewed all six of the Division's currently leased office copiers to determine if they were configured to protect confidential information processed on them.

We also reviewed the controls on entering a new employee into the state's time keeping and payroll system to ensure controls were adequate to reduce the risk of adding or paying a fictitious employee.

Our audit work was conducted from March to August of 2015. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

In accordance with NRS 218G.230, we furnished a copy of our preliminary report to the Division of Human Resource Management. On April 5, 2016, we met with Division officials to discuss the results of the audit and requested a written response to the preliminary report. That response is contained in Appendix B which begins on page 14.

Contributors to this report included:

Jeff Rauh, CISA, CIA, MBA
Deputy Legislative Auditor

S. Douglas Peterson, CISA, MPA
Information Systems Audit Supervisor

Appendix B

Response From the Division of Human Resource Management

Brian Sandoval
Governor

Patrick Cates
Director

Peter Long
Administrator

STATE OF NEVADA
DEPARTMENT OF ADMINISTRATION
Division of Human Resource Management
209 E. Musser Street, Room 101 | Carson City, Nevada 89701
Phone: (775) 684-0150 | www.hr.nv.gov | Fax: (775) 684-0122

May 31, 2016

Rocky Cooper, CPA
Legislative Auditor
Legislative Counsel Bureau
401 S. Carson Street
Carson City, NV 89701-4747

Dear Mr. Cooper:

Please accept this letter to serve as our response to the March 29, 2016 Audit Recommendation on behalf of the Department of Administration, Division of Human Resource Management regarding the information technology findings.

1. The Division of Human Resource Management (DHRM) has purchased the Oracle encryption software tool to encrypt HR Oracle databases. Enterprise IT Services Division (EITSD) has applied the tool and EITSD staff will migrate all databases according to the attached schedule. Full compliance is estimated to be complete by July 2016.

2. The Division of Human Resource Management has revised an internal checklist that supervisors must use in the event of staff turnover. This revised checklist includes discrete steps for terminating access to email as well as the associated network user account. The form has areas to notate the help desk ticket numbers and completion dates that are required to be filled out. Upon the supervisor's review and signature on the form the form is submitted to the employee's manager for review and approval. The completed and approved form is retained in the employee's agency service jacket until disposal in accordance with the records retention schedule for agency service jackets.

3. DHRM is assigning staff the task of working with EITSD to receive quarterly reports that include a listing of active user accounts on DHRM's network. The list of user accounts will be reconciled to the current employee roster to determine any needed corrections.

4. The Department ISO sends out monthly notices to agencies with the names of employees that will be due for their annual renewal of Security Awareness Training.

Employees that do not complete the training before the due date will have their security privileges temporarily suspended until training is recorded. DHRM managers will be copied on the notices to allow managers and supervisors to assist employees with scheduling the time to take the course.

5. EITSD has implemented statewide virus protection and maintains this system to ensure all subscribers are protected and updates are deployed daily. EITSD scans computers and notifies agencies of any anomalies or concerns with computers that have either been shut off or for some reason do not have a current scan on record. Appropriate instructions are given to employees to ensure their computers are scanned. The Department ISO will notify DHRM when devices are not in compliance with standard policy.

6. EITSD scans personal computers and the Department ISO is responsible to ensure all devices are up to date with virus protection and supported operating systems. Any devices that are not in compliance with security policy will be reported to agency management for correction.

7. DHRM has purchased necessary equipment and EITSD Desktop services is installing docking stations for laptops that need to be attached to the network for security and software updates and charging. Employees that use these laptops are trained in the proper procedures to attach the laptops to the docking stations for updates and charging.

8. The Department ISO is responsible to review security scans and coordinate with server administrators, network services, database administrators, and application developers to ensure all levels of security are maintained and systems and data are maintained. Any deviations or violations with security requirements will be reported to DHRM and corrective actions will be planned between DHRM and EITSD to ensure compliance.

9. The Department of Administration's internal agency IT support is provided by the Enterprise IT Services Division. Dedicated employees serve the Department including the Division of Human Resources Management under the direction of the Department Director and agency administrators. Services provided to the Department are documented on-line as the Services Catalog and DHRM receives full IT services including servers, networks, database administration, project management, desktop support, helpdesk support, and application development. The Director would provide direction to the agency administrators to take corrective actions.

10. DHRM will coordinate with agency Desktop services, Purchasing, and agency managers to ensure photocopiers are setup to prohibit the permanent storing of data and the wiping of hard drives when sent to surplus or returned to vendors.

11. DHRM will coordinate with agency Desktop services, Purchasing, and agency managers to ensure photocopiers are setup to prohibit the permanent storing of data and the wiping of hard drives when sent to surplus or returned to vendors.

Respectfully,

Peter Long

Peter Long, Administrator

CC: Jeff Rauh, Deputy Legislative Auditor, Legislative Counsel Bureau
Doug Peterson, Information System Audit Supervisor, Legislative Counsel Bureau
Patrick Cates, Director, Department of Administration
Lee-Ann Easton, Deputy Director, Department of Administration

Division of Human Resource Management Response to Audit Recommendations

	Recommendations	Accepted	Rejected
1.	Encrypt confidential personal data in Division databases at the earliest opportunity…….....	X	
2.	Implement a more effective procedure to ensure departing employees' computer accounts are disabled timely.....	X	
3.	Implement quarterly reviews of computer user accounts, as required by state security standards, to identify any former staff whose computer accounts were not disabled when they terminated employment with the Division	X	
4.	Periodically reemphasize the Division's commitment to seeing that all employees complete their annual security awareness training	X	
5.	Implement a procedure to periodically review the status of all Division computers to identify computers without up-to-date virus protection.....	X	
6.	Implement a procedure to periodically check Windows operating system software update installations to detect failed or missing updates…….....	X	
7.	Develop a Division policy and procedure requiring employees with laptop computers to periodically update the virus definitions and install Windows operating system updates timely.	X	
8.	Establish a procedure with EITS that includes providing the Division with documentation to independently verify that servers have current virus protection as well as Windows operating system updates installed	X	
9.	Ensure all Division servers maintained by EITS have current service agreements.....	X	
10.	Train staff to be aware that office copiers contain hard drives that store processed information and this information should be erased when each copier is replaced	X	
11.	Implement procedures to ensure that photocopiers are configured to not store processed data as indicated in state security standards…….....	X	
	TOTALS	11	