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)