Audit Highlights

Highlights of Legislative Auditor report on the Utilization and Security Over State Internet Sites, issued on June 24, 2004. Report #LA04-16.

Background

The Department of Information Technology (DoIT) was created in 1965 and derives its authority from NRS 242. The Department is the state's lead agency for the delivery of effective and efficient information services. All state agencies and elected officers must use DoIT for the design of their information systems, unless exempt by statute.

The Department provides Internet access for the majority of state agencies. Those agencies connect to the Internet through the state's networking infrastructure known as the Silvernet. The Silvernet links approximately 274 distinct agency networks statewide. Each of these networks corresponds to an agency's physical office somewhere in Nevada. Primary locations include Carson City, Las Vegas, and Reno/Sparks, with the remainder located throughout rural Nevada. The State has approximately 198 websites. DoIT hosts approximately 140 of these websites, with the remainder hosted by individual agencies.

Purpose of Audit

The purpose of this audit was to determine if controls are sufficient to ensure the security and integrity of the state's computer network, and information stored by agencies. Our audit included a review of controls over the State's Internet security and utilization during calendar year 2003.

Audit Recommendations

This audit report contains 15 recommendations to improve Internet security and utilization in the State. These recommendations help ensure greater security over hardware designed to limit unauthorized access to the state's information. In addition, they provide for better security over desktop computers and communication devices. Finally, the recommendations help ensure stronger controls over security incidents, prioritization of IT security planning, and backup and disaster recovery procedures.

The Department of Information Technology accepted all 15 recommendations contingent on obtaining additional staff. However, we believe the recommendations can be implemented with existing resources.

Status of Recommendations

The Department's 60-day plan for corrective action is due on September 20, 2004. In addition, the six-month report on the status of audit recommendations is due on March 21, 2005.

Utilization and Security Over State Internet Sites

Department of InformationTechnology

Results in Brief

Basic Internet security needs improvement to ensure greater protection over information stored by the State. Improvements are needed over devices that manage the flow of information as it moves throughout the state's network to prevent intrusion. These devices require regular monitoring to ensure adequate security. Another improvement needed is to prevent sensitive information from being placed on various state websites which could lead to unauthorized intrusion into the network. In addition, backup and recovery controls need to be strengthened so data is not lost after a disaster. Furthermore, the State has not prioritized its approach to implementing security procedures. These weakensses, if left uncorrected, provide opportunities for mailcious users to gain access to the state's computers, or reduce the chances of effectively recovering from a disaster. The Deparetment can overcome these weaknesses by implementing established policies and focusing greater attention on security.

Principal Findings

A router is a device that contains many rules to manage the flow of network traffic and it is designed to provide security to the state's network. The Department's router contained 12 rules that did not conform with established standards.

A firewall is a device designed to prevent unauthorized access to or from a network. Administration of the Department's firewall needs to be strengthened. First, the firewall was administered by one person who had sole authority to configure the device. This practice renders the system vulnerable to a single point of failure should this person depart the position. Second, procedures for maintaining the firewall have not been formally documented. Third, three firewall settings that did not conform to standards were not documented in a letter of exception.

DoIT maintains several computers that contain the websites of approximately 140 state agencies. These computers, called web servers, contained security weaknesses that rendered them vulnerable to attacks. First, the web servers were not located behind the protection of a firewall. Second, staff had not applied software updates or properly set some security settings. By not doing so, there is an increased risk that attackers will use the computers for unauthorized activities. For example, in November 2002 an attack resulted in approximately 60 Gigabytes of pornographic and regular movies and images being copied on a state web server. During this period, the server was being used to distribute the movies and images.

Network servers are the computers used to run an agency's network. Security settings on these servers were not in accordance with state standards. These settings resulted in a less secure network. They included passwords of insufficient length, lack of password complexity, and passwords not changed frequently. In addition, passwords could be reused too frequently, and users were not locked out after three unsuccessful login attempts.

The Department had not implemented procedures to detect unauthorized wireless access devices. These devices can circumvent other security measures such as firewalls. In addition, the current state standard for wireless networking did not include key components that would help guide state agencies in implementing this technology.

Implementation of Information Technology (IT) security has not been adequately prioritized and planned. Neither DoIT nor other agencies had received guidance on how to prioritize their efforts toward the most critical security areas. Without good detailed project planning and management techniques, it is unlikely that available resources will be most effectively used in IT Security.

Backup and recovery procedures exist to guide individuals in preserving data and restoring computer systems in the event of operational problems or a disaster. However, the Department's backup and recovery procedures are incomplete. For example, the Department has not created a contingency and disaster recovery plan, or conducted periodic testing of recovery capabilities.

For more information about this or other Legislative Auditor reports go to: http://www.leg.state.nv.us/audit (775) 684-6815.

Audit Division
Legislative Counsel Bureau