Legislative Post Audit
Performance Audit
Report Highlights

Highlights

State Agency Information Systems: Reviewing Selected Controls in Selected State Agencies (CY 2013)

Report Highlights

December 2013 ● R-13-013

Summary of Legislator Concerns

A major responsibility of agencies is to safeguard sensitive data through the implementation of security controls, including controlling agency staff access and use of the data. These controls help ensure that staff members have access only to the information needed to perform their duties and that they understand the security requirements related to their access. Currently, there is limited oversight of agencies' security controls to monitor whether these security risks are being adequately managed.

Background Information

State agencies' confidential information could be breached from outside or within an agency.

- *Hackers attempt to gain unauthorized access to confidential data from outside an agency.*
- *Confidential data could also be intentionally or inadvertently breached from within an agency.*

Agencies must protect confidential information through multiple layers of IT security including policies, software application controls, and physical security.

QUESTION: *Do Selected State Agencies Have Adequate IT Security Processes to Help Ensure that Confidential Information is Protected?*

- Three agencies had a poor security management process and none performed comprehensive risk assessments on a regular basis.
  - Three agencies had an inadequate security management process with several missing components.
  - Five of the agencies had an adequate security management process, but only one had good outcomes.

- Many agencies had a poor process to ensure staff members were using strong and secure staff passwords.
  - Five agencies had 10% or more of staff with weak passwords. *(Because agency officials had to allow us to bypass their other security controls to perform this work, it is only a test of password strength and is not an evaluation of the ease with which a hacker could access these networks.)*
  - Poor training helped explain weak passwords in agencies that had adequate passwords settings.
  - Many agencies were missing settings and had staff that were not adequately trained to ensure secure passwords.

- Six agencies did not have an adequate process to patch their servers and workstations to minimize known vulnerabilities.
  - As in past audits, agencies continue to have a significant number of software vulnerabilities.
  - Software vulnerabilities in six agencies were a result of several factors such as not scanning for vulnerabilities and misconfiguring the patching software.

- Five agencies did not have an adequate process to ensure staff were sufficiently trained in security awareness.
  - Five agencies had not trained staff in a timely manner.
  - Staff in many agencies did not fully understand several important security issues.
  - Agency officials often told us it was not an agency priority to determine how well staff understood the training provided.

- All agencies except one protected their IT infrastructure with anti-virus software.
  - One agency did not have anti-virus software installed on eight computers and did not have the software centrally managed.

- Three agencies did not have an adequate process to manage all mobile devices, and two others needed improvement in how personally owned devices were managed.
  - Three agencies lacked important controls to ensure that all mobile devices were properly restricted and that data was secured.
  - Additionally, two more agencies needed to improve how they managed personally owned mobile devices.

- Only one agency had an adequate process to continue operations in the event of an emergency.
  - As in a past audit, most agencies lacked an adequate COOP to restore operations in the event of an emergency.
  - Five agencies also were not testing their COOP on an annual basis.
  - Only KPERS sufficiently tested its COOP to ensure it could resume operations in the event of an emergency.

SUMMARY OF RECOMMENDATIONS

- We made recommendations to all eight agencies to address the specific issues at each agency.

AGENCY RESPONSE

- Seven agencies responded to the public report, and all seven agreed with the audit findings and conclusions.
- All eight agencies provided responses to their agency-specific confidential reports. Most of those agencies agreed with the audit findings and conclusions and all of them plan to implement the majority of recommendations provided in those confidential reports.

HOW DO I GET AN AUDIT APPROVED?

By law, individual legislators, legislative committees, or the Governor may request an audit, but any audit work conducted by the Division must be approved by the Legislative Post Audit Committee, a 10-member committee that oversees the Division's work. Any legislator who would like to request an audit should contact the Division directly at (785) 296-3792.

The Information Technology Executive Council has developed state security standards to help agencies protect confidential data. Almost all state agencies must comply with these standards.

We evaluated various aspects of IT security at eight state agencies:

- *Department of Administration*
- *Department for Aging and Disability Services*
- *Department for Children and Families*
- *Department of Health and Environment*
- *Kansas Attorney General*
- *Kansas Bureau of Investigation*
- *Kansas Highway Patrol*
- *Kansas Public Employees Retirement System*

This audit provides a summary of our findings across all eight audited agencies, but does not describe the security findings for individual agencies. Because those specific findings contain information that would jeopardize the agencies' security, we are keeping those findings confidential under K.S.A. 45-221(12). Audited Agencies were provided with confidential reports detailing specific problems.

Legislative Division of Post Audit
800 SW Jackson Street, Suite 1200
Topeka, Kansas 66612-2212
Telephone (785) 296-3792
Fax: (785) 296-4482
Website: http://www.kslpa.org/
Scott Frank
Legislative Post Auditor

For more information on this audit report, please contact
Justin Stowe
(785) 296-3792
Justin.stowe@lpa.ks.gov