Legislative Post Audit Performance Audit Report Highlights

Highlights

State Agency Information Systems: Reviewing Selected Controls in Selected State Agencies (CY 2012)

Report Highlights

December 2012 • R-12-012

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 applications, and physical security.

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

Findings Related To Specific IT Security Controls

- Most agencies had weak controls to help ensure strong and secure staff passwords.
  - ➢ We cracked a significant number of passwords in six agencies because staff did not create strong passwords.
  - ➢ Most agencies did not have adequate settings to help ensure passwords were adequately secured.
  - ➢ Two agencies further compromised passwords by failing to train staff that it is not acceptable to share passwords.

- Almost all agencies did a poor job of patching software vulnerabilities for both workstations and servers, ***as shown in the figure on the next page.***
  - ➢ As we have found in previous audits, most agencies had a significant number of unpatched software vulnerabilities.
  - ➢ Agencies had much more difficulty patching non-Microsoft vulnerabilities than Microsoft vulnerabilities on workstations.
  - ➢ The two agencies that performed annual vulnerability scans typically had fewer vulnerabilities on both servers and workstations.
  - ➢ The Office of Information Technology Services (OITS) recently negotiated a statewide license for vulnerability scanning software.

- Most agencies did not adequately train staff on IT security issues.
  - ➢ Seven agencies failed to provide adequate security awareness training on an annual basis.
  - ➢ Even agencies that provided regular security training had staff who did not fully understand several critical IT security risks.
  - ➢ OITS has developed centralized security awareness training but many agencies are not aware of it.

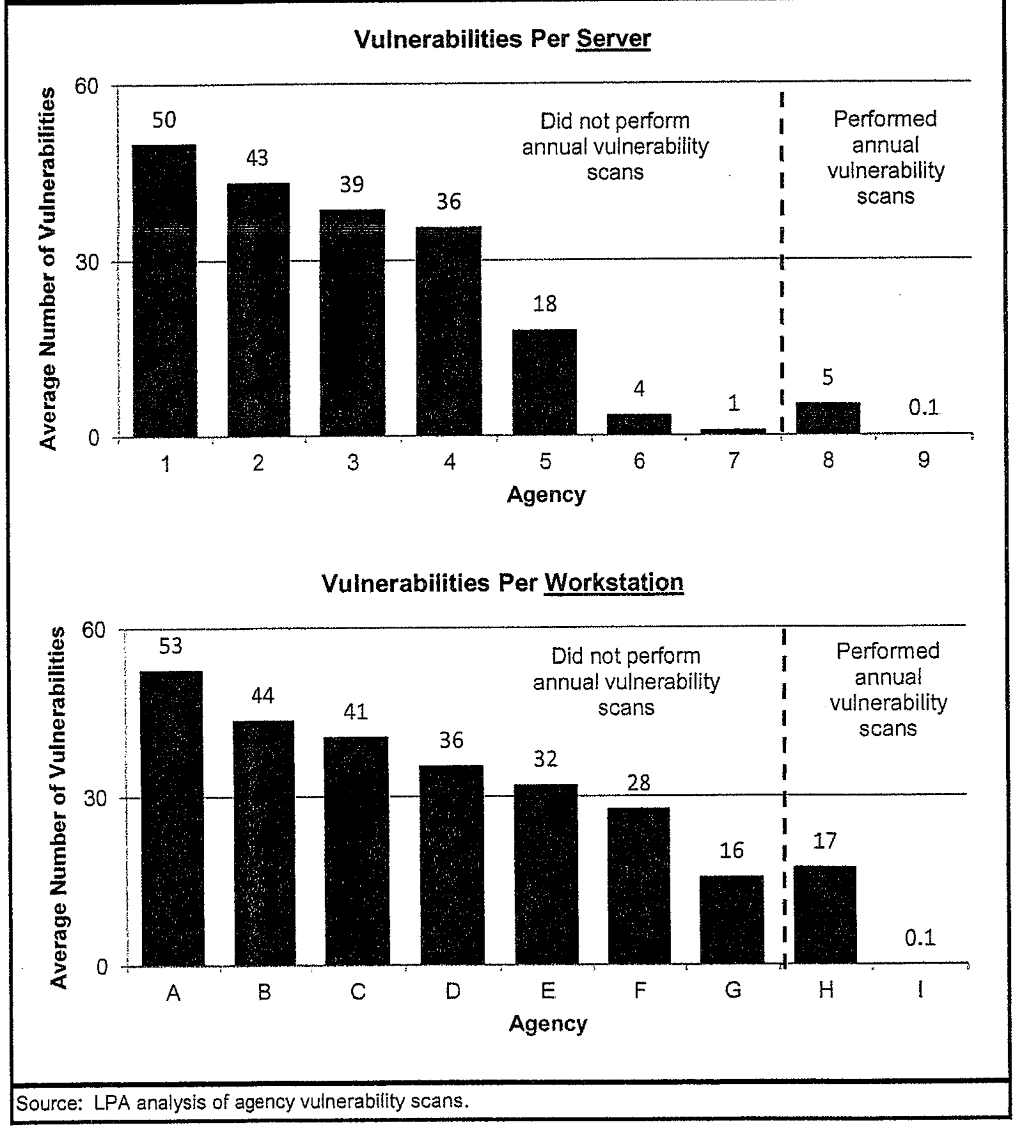
- None of the agencies had fully developed and tested a Continuity of Operations Plan.
  - ➢ Only one agency had fully developed the five sections of its continuity of operations plan that we reviewed.
  - ➢ None of the agencies routinely tested the quality and usefulness of their continuity of operations plan.

Joint Committee on Information Technology
October 21, 2013
Attachment 7

- While most agencies adequately controlled their IT inventory, four agencies were missing or had lost track of computers.
  - Five of the nine agencies were in possession of all IT hardware we looked for.
  - Three agencies had lost track of some IT equipment and one was missing four computers.
  - Four agencies did not independently check the inventory on an annual basis to ensure the agency had all required IT hardware.
  - The state's IT and accounting policies have different inventory requirements, creating confusion for several agencies.

- We found few problems with network access points, which were largely controlled by the Office of Information Technology Services.
  - Two agencies had switches located in unsecured areas that could be accessed by staff and agency guests.
  - Only one agency had any unsecured Wi-Fi access points.

Average Software Vulnerabilities for Audited Agencies' Servers and Workstations



Source: LPA analysis of agency vulnerability scans.

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 nine state agencies:

- *Board of Indigents Defense Services*
- *Department of Commerce*
- *Department of Corrections*
- *Department of Education*
- *Department of Labor*
- *Department of Revenue*
- *Department of Wildlife, Parks, and Tourism*
- *Juvenile Justice Authority*
- *State Treasurer's Office*

This audit provides a summary of our findings across all nine 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.

Findings Related To Agencies Overall Management of IT Security

- Agencies should have a comprehensive security management process to develop and enforce strong IT security controls.
  - An IT security management process includes four components that help the agency develop and enforce strong security controls.
    - A comprehensive risk assessment
    - Developing written policies and controls
    - Disseminating policies and training staff
    - Monitoring and evaluating policies and controls
  - In addition, a security-conscious management culture is a critical part of the security management process

- None of the agencies had a fully developed security management process, but all nine had at least some process components.
  - None of the agencies had conducted a comprehensive risk assessment to identify, prioritize, and resolve IT security threats.
  - None of the agencies had a complete set of policies to help establish and communicate agency accepted practices or expectations.
  - Five agencies did not effectively disseminate policies to staff that needed to be aware of them.
  - Very few agencies adequately monitored certain IT security areas to mitigate risks, including performing vulnerability scans.

- IT Security controls were far stronger at agencies where management made IT security a priority.
  - The Strongest controls were at the State Treasurer's Office, which appears to place an emphasis on the importance of IT security.

SUMMARY OF RECOMMENDATIONS

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

- The Office of Information Technology Services (OITS) should review the centralized security awareness training to ensure it effectively covers all 12 ITEC required areas. Also, communicate the availability of the training to all state agencies, as well as the ITEC mandatory requirement to train all new employees with 90 days of hire and all employees annually.

- OITS should communicate the availability of the vulnerability scanning software license to all state agencies and the ITEC mandatory requirement to conduct annual vulnerability scans.

AGENCY RESPONSE

- All nine audited agencies generally agreed with the audit findings and plan to implement the majority of recommendations provided in the agency-specific confidential reports. Also, the Office of Information Technology Services agreed with the audit findings and plans to implement the recommendations.

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.

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
Dan Bryan
(785) 296-3792
dan.bryan@lpa.ks.gov