Legislative Post Audit
Performance Audit
Report Highlights

Highlights

State Agency Information Systems: Reviewing Security Controls in Selected State Agencies (CY 2014-2016)

Report Highlights

December 2016 ● R-16-014

Audit Concerns

Kansas' Information Technology Executive Council (ITEC) has developed standards addressing various security areas. However, agencies have a significant amount of autonomy in how they develop, apply, and monitor controls in these areas. K.S.A. 46-1135 directs our office to conduct information technology audits as directed by the Legislative Post Audit Committee.

Background Information

Most state agencies maintain confidential or sensitive information. Because of this, they are consistently targeted by hackers. Insufficient security controls have led to lost or stolen information from agencies in a number of states.

Agencies should use a multi-layered approach to protect their confidential information. That way, even if one layer is compromised, the system is still protected.

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

- About two-thirds of the agencies (13 of 20) we reviewed during 2014-2016 did not substantively comply with all applicable IT security standards.

- Few agencies properly scanned their workstations and servers or patched known vulnerabilities, which increased the number of weaknesses hackers might exploit.
  - Most agencies had too many unpatched vulnerabilities.
  - Agencies often lacked the knowledge, resources, or management support to adequately scan and patch computers.
  - Without a systematic approach to identify and patch vulnerabilities, agencies leave their systems open to attack from hackers.

- Many agencies used software that was no longer supported by the vendor with security updates. Agencies also had vulnerable websites. Both of these risks can be difficult to mitigate.
  - More than half of the agencies continued to use at least some computers with unsupported operating systems or software applications.
  - At least four agencies had websites with known vulnerabilities, leading to high or critical security risks.
  - Unsupported operating systems and software as well as unsecured websites can allow attacks such as compromised websites or data breaches.

- Half of the agencies had poor access or environmental controls for their data centers, which increased their risk of data loss.
  - Agencies typically use data centers to house critical information system hardware.
  - Ten agencies did not properly restrict access to their data centers, resulting in critical or high vulnerabilities. In several instances, agency IT staff did not know who had access to the data center, or had not reviewed or updated their lists to ensure only authorized personnel had access.
  - Several agencies' data centers lacked proper environmental controls to protect against damage from fire, water, or humidity.
  - Data center controls were inadequate because agencies did not have sufficient policies or procedures and did not sufficiently consider the risks for potential compromises.
  - Poor or non-existent physical data center controls increase the risk that agencies' data center assets or information could get lost, stolen, or damaged.

- Several agencies did not adopt strong password controls which require staff to use hard-to-crack passwords.
  - Seven agencies had inadequate password settings, such as lacking sufficient password length or complexity or not locking out users who type in a wrong password too many times.
  - When fewer controls are in place, the risk increases that an agency's network could be hacked through "brute force" attacks in which hackers try many passwords until one works. Longer and more complex passwords, as well as lockout features, make such attacks much more difficult.
  - IT staff frequently cited pushback from users as the reason why sufficient password controls were not implemented.

- Several agencies did not adequately protect their network or did not sufficiently protect their systems from viruses or malware.
  - At least four agencies did not set up their firewalls properly.
  - At least six agencies had poor anti-virus protection, such as not protecting all machines or allowing users to disable their computers' anti-virus software.
  - Each of these problems creates a hole in an agency's security position because infected machines could lead to unauthorized access or data compromise.

- Several agencies did not conduct background checks or follow security protocols for departing staff.
  - At least four agencies did not background check everyone who had access to their data centers.
  - Several agencies did not have processes to retrieve badges, keys, or computers from departing staff.
  - Several agencies did not disable or deactivate building or computer access in a timely fashion.
  - Too much trust in staff, poor processes, and insufficient communication contributed to problems in these areas.
  - Improper personnel protocols increase the risk that employees might steal or otherwise compromise sensitive data.

- Many agencies did not conduct security awareness training, and our social engineering tests demonstrated a lack of understanding for security protocols.
  - State standards require new users to receive such training within their first 90 days, and for all users to receive annual refresher training.
  - About half of the agencies did not provide systematic security awareness training, resulting in significant risks.

SUMMARY OF RECOMMENDATIONS

- We made recommendations to each agency to address the specific security risks found during their audits.

HOW DO I REQUEST AN AUDIT?

By law, individual legislators, legislative committees, or the Governor may request an audit, but any audit work conducted by the division must be directed by the Legislative Post Audit Committee. Any legislator who would like to request an audit should contact the division directly at (785) 296-3792.

Agencies must use limited resources to balance their business needs against security risks. Implementing security controls takes time and may require additional IT assets.

Additional controls often can reduce speed or limit functionality, creating a tradeoff between business needs and security risks. Agencies must evaluate and understand their security risks to be able to make informed decisions.

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
Alex Gard
(785) 296-3792
alex.gard@lpa.ks.gov