Summary of Recent Data Breaches
March 16, 2015

In recent years, a number of state agencies and private businesses have been in the news because their computer networks were breached. These entities lost large amounts of highly sensitive data, including Social Security numbers, debit and credit card numbers, e-mail addresses, and other personally identifiable information. Short summaries of significant breaches and their effects are listed below.

- **South Carolina's Revenue Department.** In 2012, an employee with South Carolina's Department of Revenue clicked on an embedded link in an e-mail. That action allowed malware to invade his computer and obtain his username and password. Armed with this information, a hacker stole nearly 400,000 credit and debit card numbers. This affected more than 75% of the state's residents and cost the state $20 million for credit monitoring, security upgrades, and consultants.

- **Oregon's Breaches.** In February 2014, hackers attacked Oregon's campaign finance reporting site and central business registry for nearly three weeks. Hackers gained access to security questions for about 300,000 business accounts, which could be used for additional spoofing attacks—in which hackers use vague information to gather even more information. Similarly, in October 2014, the Oregon Employment Department was hacked. Personal information—including Social Security Numbers—for as many as 819,000 people were stolen in the breach.

- **Home Depot.** Hackers used a vendor's stolen log-on credentials to install malware on Home Depot's computer network through a hack of the company's self-checkout registers. The breach went undetected for several months, and affected 56 million credit and debit cards and 53 million e-mail addresses in the United States and Canada. As of November 2014, costs of the breach were estimated at $62 million.

- **RSA Security Company.** A 2011 breach aimed at security provider RSA's multifactor authentication tokens cost the company more than $66 million to investigate, upgrade software and hardware, and monitor customer transactions. Company officials believed the attackers wanted information it held to use in subsequent attacks against defense contractors such as Lockheed Martin.

- **Target.** In December 2013, Target revealed that hackers had stolen credit card or personal information on more than 100 million customers. For about 12 million people, both were stolen. The loss cost Target nearly $150 million in the second quarter of 2014 alone.

Prepared by Legislative Post Audit

Legislative Post Audit
Performance Audit
Report Highlights

Highlights

State Agency Information Systems: Evaluating Sensitive Datasets and IT Security Resources

Report Highlights

July 2014 • R-14-007

Summary of Legislator Concerns

Previous LPA audits have identified consistent weaknesses in state agency IT policies, procedures, and controls. Legislators were interested in a comprehensive inventory of sensitive data state agencies maintain. Additionally, legislators raised concerns regarding the state's IT security resources.

Question 1 Relevant Facts

We surveyed all state agencies to identify those that maintain sensitive data.

We also identified 21 state agencies that process a significant number of payments that could make enticing targets for external and internal attacks.

Based on the information we compiled, we assigned a risk level to all state agencies that will help focus and prioritize our future IT security audit work.

QUESTION 1: *What types of confidential and other sensitive datasets does the state maintain?*

Audit Answers and Key Findings:

- State agencies operate a variety of computer systems that must be protected.
  - Computer systems that store sensitive information can attract hackers because that information can be illegally sold or used to make money.
  - Data systems that process payments can attract hackers or fraudsters because they allow direct access to government money.
- In Kansas, most state agencies maintain computer systems that hold a variety of sensitive data or process payments.
  - Most agencies maintain personally identifiable information (PII) in addition to a variety of other sensitive data types, such as tax, health or education data.
  - More than one-third of agencies share their sensitive data with other agencies to avoid unnecessary duplication or gain operational efficiencies.
- Although the state is responsible for a vast number of sensitive or payment systems, it lacks an enterprise-level approach to IT security.
  - The state' security standard setting body, the Information Technology Executive Council (ITEC), has been largely inactive for years and its security standards are not regularly updated and enforced.
  - Although the state has taken steps to centralize many of its IT services, the state's IT security functions are almost entirely decentralized.
  - Agencies' approaches to IT security vary significantly, and these differences do not appear to be tied to different needs at each agency.
  - IT security leaders' job titles, classifications, and salaries varied significantly.
- Almost 40% (17 of 45) of the agencies that process payments or maintain large amounts of sensitive data have not had an independent evaluation of their security measures in the past three years.
- The state lacks a complete set of three-year IT plans which is required by law.
  - We noted 23 plans were missing for 2011, and agency officials told us only 49 and 26 plans were submitted for the following two years, respectively.
  - Many agencies have not submitted an annual IT plan as required, in part because agencies think they are time consuming and provide little value to them. Additionally, the Chief Information Technology Architect did not follow up on missing plans, and in one year did not send necessary templates and instructions to all agencies.
  - An incomplete set of these plans has reduced their usefulness as strategic planning tool, which is their primary purpose.

- Office of Information Technology Services (OITS) staff cannot review or compare the plans across agencies efficiently because the information is not collected in a standard format.
- IT officials at various agencies told us they spend a lot of time completing the plans but receive little feedback on them.

- Agencies' three-year IT plans have been made public despite containing sensitive security information.

QUESTION 2: Are selected state agencies' current IT security resources adequate to protect their sensitive data?

Audit Answers and Key Findings:

- The IT security reporting structures at seven of the 10 agencies create a risk that important security issues may not be communicated to top management.
  - The lead IT security official should have direct and unfiltered access to top management so they can report important security issues that affect the agency as a whole.
  - In seven agencies, the lead IT security official reported through the agency's chief information officer rather than directly to top management.
  - In one agency, this indirect reporting structure prevented top management from learning that files on the agency's network had not been backed up since November 2013.
- Three agencies' lead IT security positions were not filled with sufficiently qualified staff.
  - To be qualified as a designated lead IT security official, staff must have relevant education, experience, or security certifications.
  - One of the seven agencies with filled lead IT security positions did not meet the minimum qualifications for that role.
  - Lead IT security positions at two additional agencies had been vacant for three months or longer, leaving the security function insufficiently supervised.
- Two of the 10 agencies we reviewed lacked enough staff to perform necessary IT security tasks.
- The IT security software products agencies reported using in five security categories appeared to be adequate except for one agency that lacked software to back up its system databases and electronic files stored on its network since November 2013.

SUMMARY OF RECOMMENDATIONS

- We made a series of recommendations aimed at addressing problems with the state's three-year IT plans, and with certain agencies IT security reporting, staffing, and evaluation practices.

AGENCY RESPONSES

- Most agency officials agreed with our findings and recommendations. However, several indicated funding issues could prevent them from completing an independent evaluation of their sensitive systems. Additionally, three agencies disagreed with our recommendation to change their reporting structure, and one agency disagreed that it lacked sufficient technical staff.

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.

Question 2 Relevant Facts

Agencies have to identify and prioritize IT security threats and must deploy appropriate resources to mitigate those threats.

Our review of IT security resources focused on staffing levels, reporting structures, staff qualifications, and five security software application categories.

We evaluated 10 agencies to determine whether they had sufficient resources to protect their sensitive data or financial processes. We focused our work on agencies with large amounts of data or that processed payments. Because the agencies were judgmentally selected, our findings cannot be projected to all state agencies.

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
Katrin Osterhaus
(785) 296-3792
Katrin.Osterhaus@lpa.ks.gov