Performance Audit: City Could Better Protect Personally Identifiable Information

July 2015

City Auditor
City of Lawrence, Kansas

July 30, 2015

Members of the City Commission

The City should adopt recommended practices to better protect personally identifiable information.

The City maintains a wide range of information that can distinguish a specific individual or can be linked to specific information. All City departments have some personally identifiable information. The City maintains information in both computer systems and physical files including information on residents, customers, vendors and employees.

I make five recommendations intended to strengthen the City's ability to protect personally identifiable information. The Interim City Manager's response to the recommendations is attached.

I appreciate the cooperation and assistance I received from City staff as I completed this project.

Michael Eglinski
City Auditor

Performance Audit: City Could Better Protect Personally Identifiable Information

Table of Contents

Performance Audit: City Could Better Protect Personally Identifiable Information

Results in Brief

The City should adopt recommended practices to better protect personally identifiable information.

The City maintains a wide range of information that can distinguish a specific individual or can be linked to specific information. All City departments have some personally identifiable information. The City maintains information in both computer systems and physical files including information on residents, customers, vendors and employees.

Based on interviews and review of existing written policies and procedures, the City hasn't implemented practices recommended to protect personally identifiable information. Those recommended practices include:

- Identify and categorize information maintained.
- Minimize the collection and use of personally identifiable information.
- Develop safeguards based on the level of impact on confidentiality of the information.
- Plan to respond to a loss of information.

Losses of personally identifiable information can hurt both individuals and organizations. Individuals may suffer inconvenience, identity theft, embarrassment or blackmail. Organizations may lose public trust, face legal liability, and incur costs to remediate the loss.

The City Auditor makes five recommendations intended to strengthen the City's ability to protect personally identifiable information,

Performance Audit: City Could Better Protect Personally Identifiable Information

City should adopt recommended practices to better protect personally identifiable information

The City should implement a system to identify personally identifiable information the City maintains, develop safeguards to protect the information, and prepare to respond to a breach involving the information. The City hasn't implemented practices recommended by the U.S. Department of Commerce to protect the confidentiality of personally identifiable information.[1] Doing so would help ensure consistent, adequate protection and the ability to respond to a loss of data.

What is personal identifiable information?

Personally identifiable information refers to any information the City maintains that can distinguish a specific individual or can be linked to a specific individual. Personally identifiable information includes information in both computer systems and physical files. It includes information on residents, customers, vendors and employees. Depending on the specific information, the impact on confidentiality may be high or low.

Examples of personally identifiable information include, but aren't limited to:

- Name, such as full name, maiden name, or mother's maiden name;
- Identification number, such as social security number, driver's license number, taxpayer identification number or credit card number;
- Address information such as a street or email address;
- Personal characteristics such as a photograph or fingerprints; and
- Information that can be linked to above categories such as date of birth, employment or medical information.

The City maintains a wide range of personally identifiable information, including information about employees, residents, customers, patients and

[1] *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),* U.S. Department of Commerce, National Institute of Standards and Technology, special publication 800-122, April 2010.

vendors. The City maintains personally identifiable information in both physical and electronic formats. Every City department maintains some personally identifiable information. Some departments maintain especially sensitive information such as medical information or information related to financial transactions.

City hasn't implemented recommended practices for protecting personally identifiable information

The City hasn't implemented a system to implement the recommended practices for protecting personally identifiable information. The City Auditor interviewed people in each department and reviewed a range of policy and procedure documents to identify existing elements of recommended practice, including written policies and procedures, training, and incident response plans. Based on the interviews and document reviews, the City hasn't implemented recommended practices.

The City has some policies addressing confidentiality of information but the policies don't cover all personally identifiable information and don't fully address the recommended practices. For example, several policies at both the City and department-level address some of the recommended practices in relation to health information.

While the City hasn't implemented recommended practices, interviews show understanding of the sensitivity of some personally identifiable information and awareness of the need to protect the information. For example, Parks and Recreation described the sensitivity and importance of protecting the confidentiality of information the department has about children participating in recreation program.

Recommended practices to protect personally identifiable information

The National Institute of Standards and Technology at the U.S. Department of Commerce provides guidelines for a risk-based approach to protecting the confidentiality of personally identifiable information. Organizations should:

- Identify all of the personally identifiable information that resides in the organization.
- Minimize the use, collection and retention of personally identifiable information to what is strictly necessary.
- Categorize personally identifiable information by the level of impact to confidentiality.
- Safeguard personally identifiable information based on the impact to confidentiality. Safeguards include:
    - Policies and procedures
    - Training
    - Good security practices
- Develop plans for responding to breaches involving personally identifiable information.
- Encourage coordination within the organization, including information technology and security and legal counsel.

Following recommended practices to protect personally identifiable information helps ensure the information is protected from inappropriate access, use and disclosure. Recommended practices emphasize designing safeguards based on the specific confidentiality impacts associated with different types of information. By focusing on the impacts, safeguards can be designed to be cost effective.

City should develop plans to respond to a loss of personally identifiable information

The City hasn't developed a plan to respond to a loss of personally identifiable information. Based on audit interviews with a representative of each department, the City hasn't developed a plan to response to a breach of personally identifiable information. Response plans help to reduce the risks to both organization and individuals associated with the loss of personally identifiable information. Plans also help ensure organizations comply with legal requirements, including requirements to notify individuals when necessary.

Benefits of response planning

Planning to respond to losses of personally identifiable information help:

- Limit damage to systems
- Reduce impacts on day-to-day operations
- Improve the chances for law enforcement to identify malicious attackers

Teams that respond to data breaches can reduce costs of breaches. A recent report on breaches in the United States found that an incident response team was associated with reduced costs and was the factor that had the largest effect. Other factors that reduced costs of breaches were extensive use of encryption, involvement of business continuity management, appointing a chief information security officer, training employees, involving the governing board and having insurance.[2]

City should adopt a record retention plan

The City hasn't adopted a record retention plan. The City Clerk's Office has done some work related to developing a record retention plan, but the City hasn't adopted a record retention plan. While state law doesn't require a retention plan, it does define record retention requirements for some municipal records.[3]

Record retention plans identify and describe groups of records, establish schedules for how long to keep the records, and establish disposal procedures. Record retention plans help improve service to the public, protect records, ensure compliance with laws, improve security of confidentiality and reduce the amount of storage needed.

The Kansas State Historical Society provides recommendations for municipalities developing record retention plans.[4] Developing a plan could involve:

- Contacting the Kansas State Historical Society and other municipalities for guidance;
- Creating an inventory of records;
- Interviewing record custodians;
- Conducting legal research; and
- Appraising the records.

[2] *2015 Cost of Data Breach Study: United States*, Ponemon Institute, May 2015, page 9.
[3] K.S.A. 12-120 and K.S.A. 12-121.
[4] *Record Retention and Storage*, Kansas State Historical Society, available at: http://www.kshs.org/p/municipal-government-records-management/11346

Support from upper management and training for staff help implement a plan.

Losses of information can harm individuals and local governments

Losses of personally identifiable information can hurt both individuals and organizations. Individuals may suffer inconvenience, identity theft, embarrassment or blackmail. Organizations may lose public trust, face legal liability, and incur costs to remediate the loss. Costs for data breaches for public sector agencies average about $73 per lost record.[5]

Local governments across the country have lost data. Losses occur for a variety of reasons, such as attacks from hackers, theft or mistakes. Establishing recommended practices help address the risks of losses and help recover from a loss.

Hacker accessed personally identifiable information in Springfield

The City of Springfield, Missouri, lost personally identifiable information for over 2,000 people February 2012. A hacker accessed the information for people who visited Springfield's web page, primarily people who filed online police reports.

Springfield responded by notifying individuals whose information was accessed, offering identify theft protection, and making changes to the web page and security.

A hacker in Ohio pleaded guilty to computer fraud related to the incident and was sentenced to federal prison in 2013. The hacker pleaded guilty to illegally accessing websites of the Utah Chiefs of Police, police departments in Salt Lake City and Syracuse, and the City of Springfield.

[5] *2015 Cost of Data Breach Study: United States*, Ponemon Institute, May 2015, page 7. Costs for other sectors are higher, largely because those sectors may lose customers after a data breach.

Seattle Municipal Court employee stole personally identifiable information

An employee of the Seattle Municipal Court stole credit card numbers and other personally identifiable information from people who paid parking and traffic fines with credit cards. A bank fraud ring recruited a Seattle employee to steal the information.

The theft was identified when a police stop identified someone with numerous credit card receipts from the Seattle Municipal Court.

Following the theft, Seattle improved controls, including cash handling procedures and procedures for protecting personally identifiable information.

Berkeley staff accidentally released data in response to a records request

The City of Berkeley, California, accidentally provided employee social security numbers as part of a public records request. City staff provided a response to the request as an electronic file and removed a column identified as employee social security numbers, but didn't remove the social security number information in a second column.

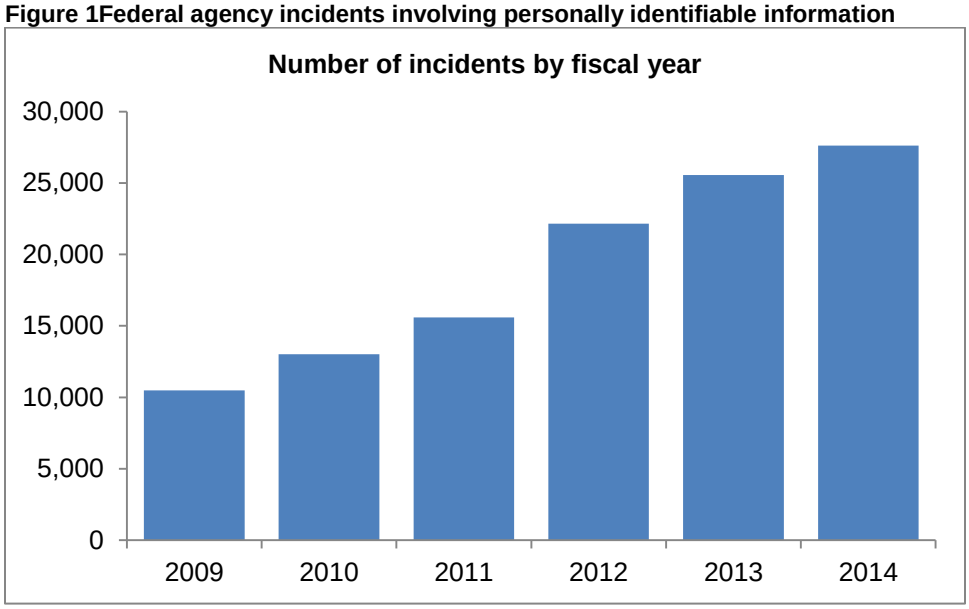
In response to the incident, Berkeley established additional controls to prevent accidental release of personally identifiable information in response to record requests.

The City has specific legal requirements depending on the nature of the personally identifiable information. For example, the City must comply with security breach investigation and notification requirements of state law that covers protection of consumer information.[6] The City must also comply with policy and training requirements of the Health Insurance Portability and Accountability Act.

Governments may be facing increasing risks related to personally identifiable information. Federal government agencies have reported an increase in cybersecurity incidents that involve personally identifiable information.

[6] K.S.A. 50-7a01 through 50-7a04.

Figure 1Federal agency incidents involving personally identifiable information



Regulations about protecting personally identifiable information may change in the near future. Data protection is an area of law still under development and rapidly changing. Changes in laws about data breaches are likely, both as legislatures create laws and as courts address those laws. Even when legal requirements don't change, expectations of residents and customers may change.

Recommendations

To strengthen the City's ability to protect personally identifiable information, the City Auditor recommends:

1. The City Manager should develop a city-wide record retention schedule.

2. The City Manager should work with the Information Technology Department and the City Attorney's Office to establish a framework for safeguarding personally identifiable information.

3. The City Manager should work with the Information Technology Department and the City Attorney's Office to provide training and communication to employees about the framework.

4. The City Manager should work with the Information Technology Department and the City Attorney's Office to establish a way to monitor how well the safeguards have been implemented.

5. The City Manager should work with the Information Technology Department and the City Attorney's Office to develop a plan to respond to a data breach.

Performance Audit: City Could Better Protect Personally Identifiable Information

Scope, methods and objectives

This performance audit was designed to address:

- Has the city implemented recommended practices to protect personally identifiable information based on the U.S. Department of Commerce National Institute of Standards and Technology framework?

To understand recommended practices for protecting personally identifiable information, the City Auditor reviewed relevant literature and state statutes. Relevant literature included:

- *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),* U.S. Department of Commerce, National Institute of Standards and Technology, special publication 800-122, April 2010.

- *Best Practices for Victim Response and Reporting of Cyber Incidents,* U.S. Department of Justice, Computer crime & Intellectual Property Section, April 2015.

- Jena Valdetero and David Zetoony, *Data Security Breaches: Incident Preparedness and Response,* 2014.

- *Recent Data Breaches Illustrate Need for Strong Controls across Federal Agencies,* U.S. Government Accountability Office testimony before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, Committee on Homeland Security, House of Representatives, June 2015.

- *Actions Needed to Address Challenges Facing Federal Systems*, U.S. Government Accountability Office testimony before the Committee on Oversight and Government Reform, House of Representatives, April 2015.

- *Cybersecurity: What the Board of Directors Need to Ask*, The Institute of Internal Auditors Research Foundation, 2014.

To understand if the City had implemented the recommended practices, the City Auditor interviewed management in each department and in several programs. The interviews focused on identifying measurable indicators of the recommended practices including written policies and procedures, designated staff with responsibility for privacy protections, employee training and incident response plans. The auditor also reviewed materials for new employee orientation and existing policy and procedure documents such as City policies on ethics, computer use, HIPAA, and open public records.

To understand risks local governments face in protecting personally identifiable information, the City Auditor reviewed information about recent data breaches in municipal governments in Springfield, MO, Seattle, WA, and Berkeley, CA. The auditor also reviewed general information about data breaches including research reports on internet security from Symantec and the cost of data breaches from the Ponemon Institute.

Because the City is subject to external audits by the Kansas Bureau of Investigation and the Kansas Highway Patrol related to criminal records, this performance audit excluded those records from the scope of work. *Performance Audit: Police Administrative Bureau – Identifying Potential Audit Topics* (October 2010) includes information on a 2008 Federal Bureau of Investigation audit of information security and a 2008 Kansas Highway Patrol audit of criminal history record information.

The City Auditor conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require planning and performing the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on the audit evidence. The City Auditor Believes that the evidence obtained provides a reasonable basis for the findings and conclusions based on the audit objectives.

The City Auditor provided a final draft of the report to the Interim City Manager on July 17, 2015 and requested a written response on or before August 3. The Interim City Manager's response is included.

Performance Audit: City Could Better Protect Personally Identifiable Information

Management's Response

City Code requires a written response addressing agreement or disagreement with findings and recommendations, reasons for disagreement, plans for implementing solutions, and a timetable for completing such activities.

City of Lawrence
CITY MANAGER'S OFFICE

DIANE STODDARD
INTERIM CITY MANAGER

City Offices
PO Box 708 66044-0708
www.lawrenceks.org

6 East 6th St
785-832-3000
FAX 785-832-3405

July 24, 2015

Mr. Michael Eglinski
City Auditor

Re: Personally Identifiable Information Performance Audit

Dear Michael,

I received your performance audit report on the City's policies and practices regarding records retention and protection of personally identifiable information. The audit report provides useful information about the City's current records management practices and how those practices may be improved going forward. Your evaluation of the City's management of personally identifiable information highlights the opportunity to establish a comprehensive framework to safeguard personally identifiable information and the importance of training City employees about the organization's responsibility to safeguard this information. The City necessarily collects and maintains a large and diverse volume of information and records. I recognize the City's responsibility to effectively manage the information and records under its care and I appreciated your recognition that City employees are sensitive to this responsibility. Effective management of personally identifiable information requires us to ensure the security of information and the City's compliance with numerous legal and regulatory requirements. Additionally, the public is entitled to access open public records, so the City must also be responsive to the public's expectation for access and transparency.

I would like to address your recommendations to establish a city-wide records retention schedule to guide the management of City records and documents. Some preliminary work on a city-wide retention schedule has been performed, and I have directed the appropriate staff to resume and complete this work. I would also like to address your recommendations regarding the establishment of a framework to safeguard personally identifiable information possessed by the City. This effort will include a training and communication strategy for employees and a monitoring strategy to evaluate the effectiveness of the safeguards. City employees are aware of the importance of protecting personally identifiable information and a comprehensive safeguarding framework will reinforce this culture of responsibility.

I agree that the City should be prepared to respond to a data breach. Information Services protects the City from hundreds-to-thousands of cyber-attacks each day, and as you reported there is a rising trend in the frequency of data breaches around the world. The Risk Management Division and Information Services Department are currently in the

process of acquiring IT insurance for the City. The insurance policy will insure the City against a data breach. The policy will also enable the City to access IT security expertise and the insurer will deploy an expert response team to the City in the unfortunate event of a data breach. I have directed the Information Services Director evaluate whether or not there is a need to conduct additional work to satisfy this recommendation.

Your recommendations call for city-wide solutions. The complexity of these city-wide solutions will require some time and resources develop and implement. I do believe there is value in addressing your recommendations and have directed the appropriate staff to begin working toward these objectives. I appreciate your analysis on this important topic.

Sincerely,

Diane Stoddard
Interim City Manager

c: Casey Toomay, Assistant City Manager
Brandon McGuire, Assistant to the City Manager
Executive Team