SPECIAL AUDIT REPORT

OF

DATABASE SECURITY
CITYWIDE

REPORT NO. 11-103

City of Albuquerque
Office of Internal Audit

Database Security – Citywide
Report No. 11-103
Executive Summary

The Office of Internal Audit (OIA) conducted a special audit of Citywide database security. The audit resulted from an *Efficiency Stewardship & Accountability* tip. As of September 19, 2011, the Department of Finance and Administrative Services (DFAS) - Information Technology Services Division (ITSD) Database Administrators (DBAs) maintain 333 databases primarily using Oracle and SQL database management systems. Some examples of service functions associated with Oracle and SQL are PeopleSoft Financials and SharePoint. The City is a decentralized entity consisting of 23 departments. Data and information maintained by these departments is also decentralized. Databases created and maintained by City departments can be stored, accessed, and shared from the following locations: a network drive, SharePoint, and City Partner Extranet.

Are databases created and maintained by City departments secured and limited only to authorized users?

Four of 35 (11%) Microsoft (MS) Access databases stored on a network drive contained confidential information. This drive is accessible to anyone with City Network access.

Thirty-three of 378 (9%) MS Excel Workbooks stored on a network drive contained confidential information.

Three of 27 (11%) SharePoint sites and one of 30 (3%) Extranet sites contained confidential information.

OIA surveyed all 23 City departments and identified 307 databases created and maintained by the departments. OIA noted:

- Seven databases stored on the C:\ drive, but never backed up to the network.
- Five databases stored on the C:\ drive, and periodically backed up to the network.
- Four databases containing confidential employee information are associated with 11 active user ids consisting of:
    - Nine assigned to individuals no longer employed by the City.
    - Two generic and not assigned to specific individuals.
- Three databases stored on the C:\ drive, and backed up to a portable electronic device instead of the network.

While conducting test work on a network drive, OIA determined that the full account numbers of four City bank accounts could be obtained by anyone who can access to the Cognos/ReportNet Public Folders.

Several of the databases and files mentioned above contained personal information. The City might incur a liability of $26,264 if it is determined that the personal information has been obtained by unauthorized individuals.

Are databases maintained by DFAS-ITSD DBAs identified and inventoried, backed-up and virus protected?

OIA identified 313 databases maintained by the DFAS-ITSD DBAs, tested a sample of 20 and determined that databases are identified and inventoried, backed-up, and virus protected.

Is access of databases maintained by DFAS-ITSD DBAs granted only to authorized individuals and limited by job function?

OIA tested a sample of 23 of 360 user ids associated with service functions classified as essential and determined:

- 23 of 23 user ids (100%) – documentation was not available indicating if training was required before access was given.
- 15 of 23 user ids (65%) – documentation was not available indicating why database access was granted.
- 4 of 23 user ids (17%) – had access that was not appropriate for the user's job function.
- 2 of 23 user ids (9%) – were still active, but the individuals they were issued to are no longer employed by the City.
- 1 of 23 user ids (4%) – was a generic user id.
- 1 of 23 user ids (4%) – enabled an operating system administrator to function as a database administrator.

OIA determined that 305 of 357 (85%) service functions have not been categorized by recovery priority.

Recommendations and management responses are included in the audit report.

City of Albuquerque

Office of Internal Audit

P.O. BOX 1293 ALBUQUERQUE, NEW MEXICO 87103

October 26, 2011

Accountability in Government Oversight Committee
City of Albuquerque
Albuquerque, New Mexico

Audit: Special Audit
Citywide Database Security
11-103

FINAL

INTRODUCTION

The Office of Internal Audit (OIA) conducted a special audit of Citywide database security. The audit resulted from an *Efficiency Stewardship & Accountability* tip.

A database is an organized collection of data for one or more purposes. Databases can result in various security requirements for Database Administrators (DBAs) as well as users. Protecting sensitive data is a major objective of any organization. Data protection or information security is protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity and availability.[1]

Security risks to databases are identified as follows:

- Unintended or unauthorized activity or misuse by DBAs, authorized users, network/systems managers, or unauthorized users or hackers.
- Performance constraints and capacity issues resulting in the inability of authorized users to use databases.
- Malware infections resulting in unauthorized access, disclosure of personal or proprietary data, deletion of or damage to the data or programs, interruption or denial of authorized database access, attacks on other systems and unanticipated failure of database services.
- Design defects and programming bugs in databases and the associated service functions and systems.

[1] - Cornell University Law School, US Code Collection, Title 44 US Code § 3542 (b) (1) (2006) as currently published by the US government. This reflects the relevant laws passed by US Congress as of 2 January 2006.

- Computer room fires or floods, static discharge, overheating, equipment failures and obsolescence resulting in physical damage to database servers.
- Loss of data caused by unauthorized access, the entry of invalid commands or data, database or system administration process errors, or sabotage.

As of September 19, 2011, the Department of Finance and Administrative Services (DFAS)-Information Technology Services Division (ITSD) Database Administrators (DBAs) maintain 333 databases, primarily using Oracle and SQL database management systems. Some examples of service functions associated with Oracle and SQL are PeopleSoft Financials and SharePoint.

The City is a decentralized entity consisting of 23 departments. Data and information maintained by these departments is also decentralized. A survey of all City departments determined there are approximately 300 databases which were developed and are maintained by City departments. These databases can be stored, accessed, and shared from the following locations:

A. The City has several *network drives*. According to DFAS-ITSD management, they were set-up to enable departments to share large amounts of electronic data with other departments. The information stored on a network drive is accessible to anyone with City network access.

B. *SharePoint* is a web-based collaboration tool which allows information sharing and document collaboration among City users. It consists of 27 individual department or division sites. SharePoint has the ability to secure and limit access to information within the individual sites, otherwise information is available to anyone with City network access.

C. *City Partner Extranet (Extranet)* consists of web-based sites similar to SharePoint, but provides the ability for individuals external to the City, such as entities in the private sector, to share information with City employees for business purposes.

AUDIT OBJECTIVES

The objectives of the audit were to determine:

- Are databases created and maintained by City departments secured and limited only to authorized users?
- Are databases maintained by DFAS-ITSD DBAs identified and inventoried, backed-up, and virus protected?
- Is access of databases maintained by DFAS-ITSD DBAs granted only to authorized individuals and limited by job function?

SCOPE

Our audit did not include an examination of all functions and activities related to databases Citywide. Our scope included security of databases during Fiscal Year 2011, real time.

This report and its conclusions are based on information taken from a sample of transactions and do not intend to represent an examination of all related transactions and activities. The audit report is based on our examination of activities through the completion of fieldwork, September 9, 2011 and does not reflect events or accounting entries after that date.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

METHODOLOGY

OIA interviewed DFAS-ITSD personnel, surveyed and interviewed departmental personnel Citywide, reviewed the network drive, local personal computer disks (C:\ drives), SharePoint/Extranet sites, survey results, and randomly sampled user identities (ids) and databases. Documents and processes reviewed include the following:

- City Information Technology (IT) Policies and Standards
- IT Governance Institute's Control Objectives for Information and related Technology (CobiT) audit guidelines
- Information Systems Control Journal, Volume 5, 2008 – Database Security Compliance and Audit
- 2010 Annual Study: U.S. Cost of a Data Breach conducted by the Ponemon Institute

FINDINGS

The following findings concern areas that we believe could be improved by the implementation of the related recommendations.

OMITTED INFORMATION

Certain sensitive information has been omitted from this report. This information has been provided to City Administration, City Council and the Accountability in Government Oversight Committee.

1. THE CAO SHOULD DEVELOP A CITYWIDE POLICY FOR THE MANAGEMENT OF SENSITIVE DATA.

OIA determined from discussions with DFAS-ISTD management during the planning stage of the audit that the City does not have specific policies in place for the management of sensitive data. DFAS-ITSD management stated that in the past the City has not considered developing specific policies for database security.

The following are results of test work performed by OIA, and serve as examples of why policies need to be in place for the management of sensitive data:

Network Drive

OIA identified and tested 35 Microsoft (MS) Access databases stored on a network drive and determined that four (11%) contained confidential information:

- Three included user information for City servers containing impact fee information.
- One contained personal information for 87 City employees.

OIA also identified 378 MS Excel Workbooks and determined that 33 (9%) contained confidential information:

- 31 included the City common fund bank account number.
- 1 contained a completed City employee's performance evaluation guide.
- 1 included personal information for 27 individuals.

City personnel did not know why this information was stored on a network drive. The MS Access database containing personal information, and the 33 MS Excel Workbooks were subsequently removed.

Cognos/ReportNet

While conducting test work of a network drive, OIA determined that the full account numbers of four City bank accounts could be obtained by anyone who could access the Cognos/ReportNet Public Folders, specifically in the Daily Bank Summary and Bank Transactions Detail reporting functions. Cognos/ReportNet is the City's financial reporting application. Public Folders do not require the individual to logon to the application.

DFAS management was not sure why the bank account numbers were included in the reporting function, but did subsequently change the format so that only the last four digits are shown when the reporting function is accessed.

SharePoint and Extranet

OIA reviewed all 27 SharePoint sites and all 30 City Partner Extranet sites, and identified three SharePoint and one Extranet sites that contained the following confidential information:

<u>SharePoint</u>

- Details of an employee incident
- User information
- Print screen showing personal information

<u>Extranet</u>

- 20 individuals' personal information

City personnel responsible for these sites were unaware that this information was accessible, agreed that access should be limited, and subsequently removed the user and personal information.

Survey

OIA surveyed all 23 City departments and identified 307 databases created and maintained by the departments. OIA reviewed the 307 databases and identified:

- Seven databases stored on the C:\ drive, but never backed up to the network. This information is not confidential, but used for business and internal department tracking purposes.
- Five databases stored on the C:\ drive, and periodically backed up to the network. This information is not confidential, but used for City business.
- Four databases containing confidential employee information are associated with 11 active user ids consisting of:
    - Nine assigned to individuals no longer employed by the City.
    - Two generic and not assigned to specific individuals.
- Three databases stored on the C:\ drive, and backed up to an external portable device instead of the network. This information is not confidential, but used for City business.

The individuals who store their databases on the C:\ drive without backing them up were unaware of the risks associated with this practice, but agreed that they should be moved to the network.

The individuals who periodically back up their databases to the network, but primarily use the C:\ drive to store them, complained of a slow network connection and processing speed.

One individual stored all of her data on the C:\drive, and did not back up the information to the network. This individual subsequently moved everything to the network after OIA informed her

Survey
that her information was at risk of being accessed by unauthorized individuals, or lost if her C:\drive crashed. The City Information Technology Electronic File and Document Storage Standard states that files and documents shall not be stored on local personal computer disks (e.g., on the C:\ drive). All user-generated files should be stored on the City network servers which are automatically and routinely backed up.

CobiT's control practices suggest defining and implementing a policy to protect sensitive data.

The potential cost for a data breach caused by negligence is $196/record based on a 2010 Annual Study: U.S. Cost of a Data Breach conducted by the Ponemon Institute. The Ponemon Institute conducts independent research on privacy, data protection and information security policy. Their goal is to enable organizations in both the private and public sectors to have a clearer understanding of the trends in practices, perceptions and potential threats that will affect the collection, management and safeguarding of personal and confidential information about individuals and organizations. Ponemon Institute research informs organizations on how to improve upon their data protection initiatives and enhance their brand and reputation as a trusted enterprise.

The City might incur a liability of $26,264 if it is determined that the 134 instances of personal information have been obtained by unauthorized individuals as a result of a data breach:

Source	**Instances**	**Cost per record**	**Total Cost**
MS Access	87	$196	$ 17,052
MS Excel	27		$ 5,292
Extranet	20		$ 3,920
Total	**134**		**$ 26,264**

RECOMMENDATION

The CAO should:

- Develop a City wide policy for the management of sensitive data.
- Ensure the policy is regularly communicated (i.e., New Employee Orientation, City eweb, quarterly communications).
- Regularly remind City users not to store data on the C:\ drive.

RESPONSE FROM THE CAO

"ITSD will develop a city wide policy for the management of sensitive data. Upon the adoption of the policy the City will also create procedures on how this policy will be enforced and how City employees will be notified both initially and on-going."

ESTIMATED COMPLETION DATE

"Policy to be written and promulgated by November 30, 2011."

2. THE CAO SHOULD ENSURE THAT ALL CITY DEPARTMENTS ARE INVOLVED IN THE PROCESS OF IDENTIFYING THE RECOVERY PRIORITY OF ALL CITY SERVICE FUNCTIONS.

OIA determined that 305 of 357 (85%) service functions have not been categorized by recovery priority while reviewing databases maintained by the DFAS-ITSD DBAs. A service function is a computer application such as PeopleSoft Human Resources that is owned by a department, such as Human Resources and maintained by DFAS-ITSD.

According to DFAS-ITSD management, only systems considered essential for ongoing City business in the event of a disaster have been categorized by recovery priority. DFAS-ITSD management also mentioned that none of the City departments, who are the business process owners of the service functions, participated in this process. It is not clear to DFAS-ITSD if all service functions essential for ongoing City business have been identified.

CobiT control practices suggest defining and implementing a process to clearly identify sensitive data as well as communicating and agreeing on the classification of data with the business process owners.

If City departments are not involved in the process of identifying the recovery priority of service functions, data that is critical to on-going City operations might not be clearly identified. Business objectives might not be met and confidence of our citizens, customers, taxpayers, ratepayers and bondholders might not be maintained.

RECOMMENDATION

The CAO should ensure that all City departments are involved in the process of identifying the recovery priority of all City service functions.

RESPONSE FROM THE CAO

"The Administration agrees with the finding.

"ITSD will create a process (through a project plan) to ensure that all City Departments have identified their priority of service functions through a Business Impact Analysis (BIA). A Business Continuity Plan (BCP) will be created for each service function. This will be included in the Enterprise Architecture (EA) Program that is being instituted by ITSD.

"The BCP will be used by ITSD to determine the direction that IT will take for both IT BCP and Disaster Recovery for the City business functions."

ESTIMATED COMPLETION DATE

"Recovery priority project to begin in October 2011 and be completed by March 2012."

3. DFAS-ITSD SHOULD ENSURE THAT WRITTEN POLICIES AND PROCEDURES ARE IN PLACE AND FOLLOWED FOR THE GRANTING AND TERMINATING OF DATABASE ACCESS.

OIA identified 360 user ids that have access to databases associated with service functions that are classified as being essential to City business. OIA tested a sample of 23 user ids and determined:

- 23 of 23 user ids (100%) – documentation was not available indicating if the user was required to have training prior to being granted database access.
- 15 of 23 user ids (65%) – documentation was not available, such as a Help Desk Ticket, indicating why they were granted database access.
- 4 of 23 user ids (17%) – had access that was not appropriate for the user's job function.
- 2 of 23 user ids (9%) – were still active, but the individuals they were issued to are no longer employed by the City.
- 1 of 23 user ids (4%) – was a generic user id.
- 1 of 23 user ids (4%) – enabled an operating system administrator to have the same functional role as a database administrator. The roles of operating system and database administrator should be separate.

DFAS-ITDS management stated that the reason for these issues seems to be that many of the processes were previously implied or assumed, but not in writing; and therefore they were not consistently followed.

CobiT control practices suggest establishing a set of user account management procedures to address requesting, establishing, issuing, suspending, modifying and closing user accounts.

If policies and procedures are not in place for database access, data which is essential to City operations might be altered, misused, or destroyed by an unauthorized individual.

RECOMMENDATION

DFA- ITSD should ensure that written policies and procedures are in place and followed for the granting and terminating of database access.

RESPONSE FROM DFAS

"The department agrees with the finding.
"ITSD will determine a process and procedure to appropriately provision and de-provision accounts and privileges to the City's databases."

ESTIMATED COMPLETION DATE

"Project to begin in October 2011 and be completed by February 2012."

CONCLUSION

This audit will help the CAO and DFAS-ITSD identify and implement controls, policies, and procedures for the management of confidential and sensitive City data.

We appreciate the assistance and cooperation of DFAS-ITSD and other City department personnel during the audit.

Senior Information Systems Auditor

REVIEWED:

Internal Auditor

APPROVED:

Carmen Kavelman, CPA, CISA, CGAP
Director, Office of Internal Audit

APPROVED FOR PUBLICATION**:**

Chairperson, Accountability in Government
Oversight Committee