MANAGEMENT AUDIT REPORT

OF

SECURING CRITICAL DATA CITYWIDE

REPORT NO. 09-106

City of Albuquerque
Office of Internal Audit and Investigations

Securing Critical Data – Citywide
Report No. 09-106
Executive Summary

Background

The Office of Internal Audit and Investigations (OIAI) conducted a Citywide performance audit of the security and storage of electronic user-developed documents. This audit was included in the fiscal year (FY) 09 approved audit plan.

The protection of City of Albuquerque (City) documents from unauthorized access, modification, and deletion is critical to business operations as well as the City's reputation. The City must comply with federal laws such as the Privacy Act of 1974 and the Health Insurance Portability and Accountability Act (HIPAA) which require that personal and sensitive health care information be protected from unauthorized access. The City must also provide security to decrease the risk of identity theft. Due to the increase in identify theft some states have passed laws that monetarily penalize organizations that do not adequately protect private information. New Mexico currently does not have this type of law but courts throughout the nation have determined that theft of electronic data is a foreseeable threat and that organizations must provide adequate security.

Data is accidentally or intentionally disclosed most often through an unprotected desktop personal computer (PC), laptop, or USB flash drive. The consequences of unauthorized disclosure of private or sensitive City information may include: loss of reputation; loss of community trust; loss of focus from organization goals and objectives; and legal liability.

Objectives:

Are Information Technology (IT) Policies and Standards for the securing of user-developed electronic data followed?

Is access to critical user-developed data appropriately restricted to authorized personnel?

Are user-developed documents saved on local hard drives or external storage media?

- Twenty-five out of 53 (47%) employees tested were not aware of the Department of Finance and Administrative Services/Information Services Division (DFAS/ISD) Electronic File and Document Storage Standard (Document Storage Standard).
    - The SWMD network does not display the notice to employees that is displayed on the Novell network which communicates the Document Storage Standard.
- Fifteen out of 53 (26%) employees tested were saving all user-developed documents on their local hard drive (C: drive).

- Thirteen out of 53 (25%) of employees tested used a USB flash or thumb drive to save City documents on a temporary basis.
- All employees tested had access to network drives restricted to the user or their department.

Recommendations: The CAO should:

- Implement measures to ensure that City policies and standards regarding the security and storage of user-developed documents are effectively communicated.
- Ensure City documents are periodically reviewed, securely stored, and backed up on a regular basis.

SWMD should post a notice to employees, similar to the one displayed on the Novell network, when users logon to the SWMD network.

Objective: Is the server/directory that stores critical data backed up regularly and stored in a secure area?

- Aviation's backup software is not configured to automatically perform backup of user-developed documents. Backup media is not stored in a fireproof media safe or rotated offsite.
- ABQ Ride temporarily halted routine backups, does not store backup media in a fire-rated safe or rotate media offsite.

Recommendations: Aviation should:

- Configure their backup software to automatically perform backups of file servers that store user-developed documents on a daily incremental and full weekly schedule.
- Back up documents to a removable external hard drive that can be rotated offsite.
- Store backup media onsite in a fireproof media safe, rotate backup media to a secure offsite facility and store in a fireproof media safe.

ABQ Ride should:

- Perform routine backup activities.
- Store backup tapes onsite in a fireproof media safe, rotate backup media to a secure offsite facility and store in a fireproof media safe.

During our fieldwork, we noted no exceptions for the following objective:

Are user-developed documents regularly reviewed for processing integrity, as well as completeness and accuracy of data?

Management responses are included in the audit report.

City of Albuquerque

Office of Internal Audit and Investigations
P.O. BOX 1293 ALBUQUERQUE, NEW MEXICO 87103

July 29, 2009

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

Audit: Management Audit
Securing Critical Data - Citywide
09-106

FINAL

INTRODUCTION

The Office of Internal Audit and Investigations (OIAI) conducted a Citywide management audit of the security and storage of electronic user-developed documents. This audit was included in the fiscal year (FY) 09 approved audit plan.

The protection of City of Albuquerque (City) documents from unauthorized access, modification, and deletion is critical to business operations as well as the City's reputation. The City must comply with federal laws such as the Privacy Act of 1974 and the Health Insurance Portability and Accountability Act (HIPAA) which require that personal and sensitive health care information be protected from unauthorized access. The City must also provide security to decrease the risk of identity theft. Due to the increase in identify theft some states have passed laws that monetarily penalize organizations that do not adequately protect private information. California Civil Code 1798.80-1798.84 states that if organizations have reckless violations, such as repeated theft or disclosure of private information, civil penalties of $3000 per violation or record can be imposed. New Mexico currently does not have a similar law but courts throughout the nation have determined that theft of electronic data is a foreseeable threat and that organizations must provide adequate security.

Data is accidentally or intentionally disclosed most often through an unprotected desktop personal computer (PC), laptop, or USB flash drive. The consequences of unauthorized disclosure of private or sensitive City information may include: loss of reputation; loss of community trust; loss of focus from organization goals and objectives; and legal liability.

The City has Information Technology (IT) Policies and Standards as well as Personnel Rules and Regulations in place for the security of documents. The Department of Finance and Administrative Services/Information Systems Division (DFAS/ISD) provides City computer users access to secure restricted network folders that are routinely backed up. It is ultimately the responsibility of each computer user to follow DFAS/ISD procedures to safeguard their documents.

AUDIT OBJECTIVES

The objectives of the audit were to determine:

- Are IT Policies and Standards for the securing of user-developed electronic data followed?
- Is access to critical user-developed data appropriately restricted to authorized personnel?
- Is the server/directory that stores critical data backed up regularly and stored in a secure area?
- Are user-developed documents regularly reviewed for processing integrity, as well as completeness and accuracy of data?
- Are user-developed City documents saved on local hard drives or external storage media?

SCOPE

Our audit did not include an examination of all functions and activities related to the security of City data. Our scope was limited to the above objectives for the period of FY09.

This report and its conclusions are based on information taken from a sample of network accounts and does not intend to represent an examination of all network account users. The audit report is based on our examination of activities through the completion of fieldwork, April 8, 2009 and does not reflect events 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. This audit was also conducted in accordance with IT Governance Institute's Control Objectives for Information and related Technology (CobiT) audit guidelines. The IT Governance Institute is a standard setting organization for information systems auditing. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

METHODOLOGY

OIAI reviewed City IT Policies and Standards pertaining to the storage and security of City data and researched best practices and authoritative IT guidance on the security and storage of critical data. Following are documents reviewed and used as criteria in the audit:

- DFAS/ISD Policy –Information Technology Protection
- DFAS/ISD Standard – Electronic File and Document Storage
- Personnel Rules and Regulations – 301.13 City Records and Accounting
- Personnel Rules and Regulations – 301.16 Privileged Information
- CobiT Control Objective PO2.3 – Data Classification Scheme
- CobiT Control Objective PO2.4 – Integrity Management
- CobiT Control Objective DS11.6 – Security Requirements for Data Management
- CobiT Control Objective DS4.9 – Offsite Backup Storage
- CobiT Control Objective DS11.5 – Backup and Restoration
- CobiT Control Objective PO7.4 – Personnel Training
- IT Control Objectives for Sarbanes-Oxley - End User Computing Control Guidance

OIAI interviewed personnel in DFAS/ISD, who administer the City's core network, and departments that administer their own networks: ABQ Ride Department (ABQ Ride), Aviation Department (Aviation), Albuquerque Fire Department (AFD), Albuquerque Police Department (APD) and Solid Waste Management Department (SWMD). OIAI obtained an understanding of backup procedures for network file servers storing user developed documents as well as user access to network drives. OIAI observed backup software settings to confirm that data is backed up on a regular basis and observed backup media to ensure that it is stored securely and protected against environmental threats.

FINDINGS

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

1. THE CHIEF ADMINISTRATIVE OFFICER (CAO) SHOULD ENSURE THAT CITY POLICIES, STANDARDS, AND PROCEDURES REGARDING THE STORAGE AND SECURITY OF DATA ARE EFFECTIVELY COMMUNICATED AND FOLLOWED.

   OIAI selected a statistical sample of 53 network user accounts from a population of 4,888 to determine if current City policies and procedures were operating effectively. For each network user account OIAI:

- Interviewed the employee to obtain an understanding of their knowledge of existing City policies and standards regarding data security and storage and determine if external storage media is used to save documents;
- Observed where employees stored user-developed documents;
- Observed network drive mappings and security restrictions for their network access.

OIAI determined the following from this test work:

- Twenty-five out of 53 (47%) employees were not aware of the DFAS/ISD Electronic File and Document Storage Standard (Document Storage Standard)
    - Four employees were only signing onto their workstation and were unaware that they had access to network drives.
    - Two SWMD employees were not aware of the Document Storage Standard. The SWMD network is not administered by DFAS/ISD and does not display the notice to employees that is displayed on the Novell network which communicates this Standard. SWMD IT personnel currently take an image of SWMD user's PCs once a month to aid in the recovery of a PC if a problem occurs. While this is a good practice, it should not take the place of saving documents to a network folder that is routinely backed up.
- Fifteen out of 53 (28%) employees were saving user-generated documents on their local hard drive (C: drive).
- Thirteen out of 53 (25%) employees use a USB flash or thumb drive to save City documents on a temporary basis.
- All employees had access to network folders to save documents. Often these are mapped as the M: or X: drive.

The Document Storage Standard states that user-generated documents should be stored on network-attached file servers configured for routine backup and recovery operations. Files and documents shall not be stored on the local hard disk or removable media (e.g. CDs/DVDs, USB thumb or flash drives). DFAS/ISD currently communicates this standard on a notice to employees displayed to users when they log onto the Novell network and it is included on the City Employee Web, (eweb.cabq.gov), accessible to all employees.

The local hard drive or flash drive is not as secure as the network drive and are not backed up on a regular basis. Documents saved on local drives or flash drives have an increased risk of unauthorized access, modification and disclosure because anyone with access to the PC, laptop, or flash drive has access to documents stored on them. In addition, if the local hard drive crashes or becomes infected documents may not be recoverable. Network drives or folders are password

protected and restricted to a specific user or user group based on job responsibilities. User groups are logical groupings of employees, usually grouped by department or division.

Employees that were saving documents to their local drive or thumb drive were unaware of the security risks or the benefits of saving documents to the network drive. Some users were uncertain which network drives to save their documents.

The DFAS/ISD IT Protection Policy states that information must be protected according to its sensitivity, criticality, and value regardless of the media on which it is stored and that all employees have a responsibility to protect information from unauthorized access, modification, disclosure, and destruction, whether accidental or intentional. This policy is on the City Employee Web.

Personnel Rules and Regulations section 301.13 states that all City records be prepared factually and accurately. It is the personal obligation of the employee completing such records as well as the supervisor to ensure that such records are accurate and comply with federal, state and City requirements. Section 301.16 states that employees shall protect privileged information to which they have access in the course of their official duties.

CobiT Control Objectives recommend that an approach for the communication of policies and procedures be supported by appropriate awareness training to ensure transparency and understanding of the policies.

RECOMMENDATIONS

The CAO should implement measures to ensure City policies and procedures regarding data security and storage are effectively communicated. Measures may include:

- Addition of a data security section to the New Employee Orientation to cover IT policies and standards.
- Expansion of the IT Certification Test to include information/questions pertaining to data security and storage.

The CAO should ensure that all City documents are periodically reviewed, securely stored, and backed up on a regular basis. Management Citywide should take an active role to ensure documents used in their operations are identified, periodically reviewed, and stored securely on the network. Even though DFAS/ISD provides access to secure network folders, it is each employee's responsibility to use these tools.

SWMD should post a notice to employees on their network, similar to the one displayed on the Novell network, to communicate the DFAS/ISD Document Storage Standard.

RESPONSE FROM CAO

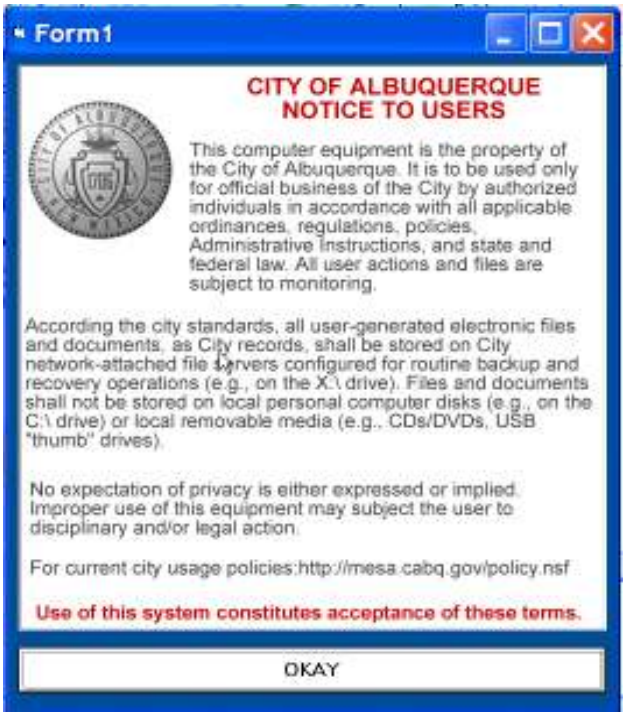
"The CAO concurs with these recommendations.

- ***HR and DFAS/ISD have begun a collaborative effort to include data security information in the NEO with an anticipate date of December 2009.***
- ***The IT Certification Test will be expanded to include information/questions pertaining to storage of City data file servers that are regularly backed up by January 2010.***

The enhancement of communicating to employees through New Employee Orientation and inclusion of this information in the IT Certification test will provide an annual reminder to all employees."

RESPONSE FROM SWMD

"SWMD concurs with this recommendation. Prior to the conclusion of the "Securing Critical Data" Audit the department posted and displayed the following message:"



2. AVIATION SHOULD CONFIGURE SOFTWARE TO AUTOMATICALLY PERFORM BACKUPS OF USER-DEVELOPED DOCUMENTS AND STORE BACKUP MEDIA IN A SECURE OFFSITE LOCATION.

OIAI interviewed Aviation IT personnel to obtain an understanding of their backup procedures and observed screen shots from the file server showing backed up documents for each division within Aviation.

The backup software is not configured to recognize all servers on the Aviation network. The fileserver that stores user-developed data is not automatically backed up on an incremental daily and full weekly schedule. The Aviation IT manager manually copies user data files and databases once a week to a backup file server, so any documents created or modified and subsequently deleted within the same week are not recoverable. If the two Aviation IT managers are not available, manual backups may be overlooked or if less experienced personnel perform this function some folders may not get copied to the backup server.

Aviation does not provide offsite storage of backup media. The production servers and the backup server are located in the same server room and are subject to the same risks. Aviation prefers to backup data to disk rather than tape and currently no offsite storage procedures for backup media are in place. If a disaster impacts the server room both the production and backup data may be unavailable to recover Aviation systems in a timely manner. The IT manager reported that a disaster recovery site is planned as part of the Aviation communications center remodel scheduled to begin in FY10.

CobiT Control Objectives provide guidelines for the regular backup of data, data recovery testing, and offsite storage of backup media. Procedures for routine backup of data and data recovery testing should be defined. Daily incremental or differential backups as well as weekly full backups should be performed to ensure recoverability of data. Backup media should be adequately protected both on and offsite. Secure offsite storage of backup media ensures the recoverability of data in the event of a disaster.

RECOMMENDATION

Aviation should implement measures to ensure all user-generated documents are backed up on a regular basis and backup media is secure. Measures may include:

- Configure backup software to automatically backup file servers that store user-developed documents on a daily incremental and full weekly schedule.
- Backup documents to a removable external hard drive that can be rotated offsite.

- Backup media should be stored onsite in a fireproof media safe and rotated offsite to a secure location and stored in a fireproof media safe.

RESPONSE FROM AVIATION

"Aviation concurs with these recommendations. Data restores are being performed and have been successful. As a temporary measure Aviation is in the process of identifying a secondary back-up server for data which will be located offsite including a software program that will be set to back-up files on a regular basis, to be completed by September 2009. Double Eagle II Airport or Airfield Maintenance has been identified as potential offsite locations where media can be stored in fireproof media safe.

"Upon completion of the Communication Center remodel, 2010 a NetApp server will be incorporated that will allow complete back-up technique for databases, user data and system mirroring."

3. ABQ RIDE SHOULD PERFORM BACKUP ACTIVITIES AND STORE BACKUP MEDIA IN A SECURE OFFSITE LOCATION.

OIAI interviewed ABQ Ride IT personnel to obtain an understanding of their backup procedures and observed screen shots from the backup system to confirm scheduling of routine backups. OIAI also observed the backup system's tape library and media stored in the server room.

ABQ Ride has backup software in place and was performing daily incremental and weekly full backups until it was halted temporarily due to communication issues within the department. ABQ Ride is storing backup tapes in a tape library within the server room and does not rotate tapes offsite.

ABQ Ride operations are at risk because current data and systems will not be recoverable due to the lack of regular backups. Production and backup data are currently subject to the same risks since they are stored in the same room. If a disaster impacts the server room, data and systems would not be recoverable because backup media is not rotated offsite.

CobiT Control Objectives provide guidance on data backup, recovery, and storage. Procedures for the regular backup of data as well as on and offsite storage should be defined. Backup media should be adequately protected both on and offsite. A fireproof media safe or cabinet would provide protection against environmental threats and restrict access to backup media. Offsite

storage would provide another level of safety and enable recovery of operations at a different location if the data center is not available.

RECOMMENDATION

ABQ Ride should implement measures to ensure all user-generated documents are recoverable and that backup media is secure. Measures may include:

- ABQ Ride performing regular backup and data recovery activities,
- Backup media should be stored onsite in a fireproof media safe and rotated offsite to a secure location and stored in a fireproof media safe.

RESPONSE FROM ABQ RIDE

"ABQ Ride concurs with these recommendations. A listing of data stores that require back-up was reviewed and revised in mid-May 2009. Several back-up software licenses have been secured and the software had been configured and backups are being currently written to tape. Additional backup software licenses will be acquired by mid-July 2009.

"ISD division has made space and a fireproof vault available and tapes are currently being stored off site. In mid June 2009, a backup server rack was relocated to Pino Yards."

CONCLUSION

City documents are at risk of being accidentally or intentionally disclosed, modified, or deleted because documents are not being stored securely on network-attached file servers. DFAS/ISD provides guidance through Policies and Standards, access to restricted network drives and regularly backs up data residing on these network drives. Ultimately the protection of data resides with the employee. Computer users, together with department management, are the owners of City data and must determine what is critical to their operations and ensure that it is securely stored in a location that is regularly backed up.

We appreciate the assistance and cooperation of DFAS/ISD, ABQ Ride, Aviation, AFD, APD, and SWMD personnel during the audit.

_____
Senior Information Systems Auditor

REVIEWED:

_____ _____
Audit Manager Internal Auditor

APPROVED: APPROVED FOR PUBLICATION**:**

_____ _____
Carmen Kavelman, CPA, CISA, CGAP Chairperson, Accountability in Government
Director Oversight Committee
Office of Internal Audit & Investigations