



Audit Department

500 S Grand Central Pkwy Ste 5006 • PO Box 551120 • Las Vegas NV 89155-1120
(702) 455-3269 • Fax (702) 455-3893

Angela M. Darragh, CPA, CFE, CISA, Director

May 6, 2014

Mr. Don Burnette
Clark County Manager
500 South Grand Central Parkway, 6th Floor
Las Vegas, Nevada 89106

Dear Mr. Burnette:

In accordance with our annual audit plan, we conducted an audit of Clark County Information Technology Email Service. The audit reviewed procedures for the period from September 1, 2013 to November 18, 2013.

The objective of our audit was to determine whether security over email service is adequate to safeguard against threats and unauthorized access.

To accomplish our objectives, we reviewed all users identified all active users with Clark County domain. We determined validity of the accounts by determining active employment and vendor status. We detail tested 35 accounts by reviewing user accounts with Information Technology. We reviewed exchange system scans, email policies, network rules, administrator access, back-ups and replications, email storage, change controls, and antivirus software and updates.

Security over email service is reasonably adequate to safeguard against external threats. However, Information Technology does not have sufficient processes in place to prevent unauthorized access from former users of email, as user accounts that include employees, vendors, "Send As", and other external users are not validated on a consistent basis. Many employees that have terminated employment with the County continue to have active email service and potential access to the network and other County information systems resources. We consider this a high risk to County systems and to the validity of County communications. Identifiers such as employment personnel numbers or vendor account numbers are not consistently maintained in email account data to verify user. Additionally, the exchange system replications and back-ups are also not tested to determine that a successful recovery is possible. Lastly, emails are retained indefinitely with storage space use of 14.4 Terabytes in production, 132 Terabytes of replications, and 22 Terabytes for archives.

A draft report was provided to the Chief Information Officer for comment and his response is included. We appreciate the cooperation and assistance provided by the Department of Information Technology.

Sincerely,

Angela M. Darragh, CPA
Audit Director



AUDIT DEPARTMENT

Audit Report

Information Technology Email Service

May 2014

Angela M. Darragh, CPA, CISA, CFE
Audit Director

AUDIT COMMITTEE:

Commissioner Steve Sisolak

Commissioner Chris Giunchigliani

Commissioner Lawrence Weekly

TABLE OF CONTENTS

BACKGROUND	1
OBJECTIVES, SCOPE, AND METHODOLOGY	1
RESULTS IN BRIEF	2
DETAILED RESULTS	3
Many Active Email Accounts Not Valid with Potential Network and Mainframe Access (HIGH)	3
Inconsistent Identification of Internal and External Users (HIGH)	5
Emails Retained Indefinitely (HIGH).....	6
“Send As” Names No Longer Valid (MEDIUM)	7
Passwords Not Required and Never Expire (MEDIUM).....	7
Recovery of Exchange System Not Tested (LOW).....	8
MANAGEMENT RESPONSE	9

BACKGROUND Clark County (County) uses Microsoft Outlook to electronically communicate internally and externally. It is a vital part of County communications. The County established directives to safeguard communications and data shared through this tool. Information Technology (IT) is ultimately responsible for maintaining an operative email service and security over the service.

County Departments are responsible for notifying IT to initially authorize or disable email service accounts. Information Technology activates and deactivates accounts. Users of the County email service must also be granted network access, as servers for email service reside within the County's information technology framework. Users of the County email service may include external users such as consultants, vendors, and other organizations. At the time of the audit, there were in excess of 5,400 email users.

Information Technology has moved to replication processes as a means of back-up for email data and archives, as opposed to tape back-ups. Replicas exist on County servers and at vendor facilities.

Email service is also accessible through the internet and the Outlook Web App.

OBJECTIVES, SCOPE, AND METHODOLOGY The objective of our audit was to determine whether security over email service is adequate to safeguard against threats and unauthorized access. Note that we did not include a review of mobile device access. Clark County is in the process of developing a policy for personally owned devices and associated controls over mobile device access to emails.

To achieve our audit objectives we met with the team of information technology professionals that are responsible for overseeing and maintaining email service. We obtained an understanding of the configuration of servers and software needed to provide secure and operational email service, archiving, and backups. We reviewed Clark County Directives in regards to email service security and access. We observed, obtained screen shots, and examined configuration settings of network rules. We obtained and examined scans of external and internal servers and verified threat remediation. We obtained and reviewed file types of attachments allowed, settings and expirations of anti-spam and anti-virus software, email service change forms for proper authorizations, and email storage capacity and use. We obtained a listing of all users with the County domain and determined whether users were active employees. We then detail tested 50 of these user accounts and five vendor accounts. We reviewed all generic account users for reasonableness of active status. Administrator access and permissions were then reviewed for

current active employment status and appropriateness given job positions.

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.

Our procedures were performed for the period from September 1, 2013 to November 20, 2013. The last date of fieldwork was January 8, 2014.

RESULTS IN BRIEF

Security over email service is reasonably adequate to safeguard against external threats, and the use of generic email accounts, except for four test accounts, and administrators' access and permissions appeared reasonable. However, Information Technology does not have sufficient processes to prevent unauthorized access from former users of the email service as user accounts that include employees, vendors, "Send As", and other external users are not validated on a consistent basis. Many employees that have terminated employment with the County continue to have active email service. Identifiers such as employment personnel numbers or vendor account numbers are not consistently maintained in email account data to verify users.

We also found that emails are retained indefinitely, as Clark County management and Information Technology has used this service as a place of record and has not been able to reasonably identify and classify emails in order to implement destruction directives established by Clark County in accordance with Nevada Revised Statutes 239. This leaves the County susceptible to liability for historical and confidential information that should have been destroyed in accordance with minimum standards of record retention. Storage space continues to grow, and is currently at over 14.4 terabytes. Replication storage is considerably larger.

While risk of historical and confidential information being inappropriately shared and miscommunication occurring is greatly increased due to the lack of adequate controls over active accounts, the greater risk is that these users may maintain internal network and application access.

Each finding is discussed in more detail below, and includes a risk ranking high, medium, or low for the finding. This ranking is based on our assessment of the

probability and potential impact of the concern to one or more of the following areas:

- Reputation and Customer Confidence
- Financial
- Productivity
- Safety and Health
- Fines and Legal Penalties

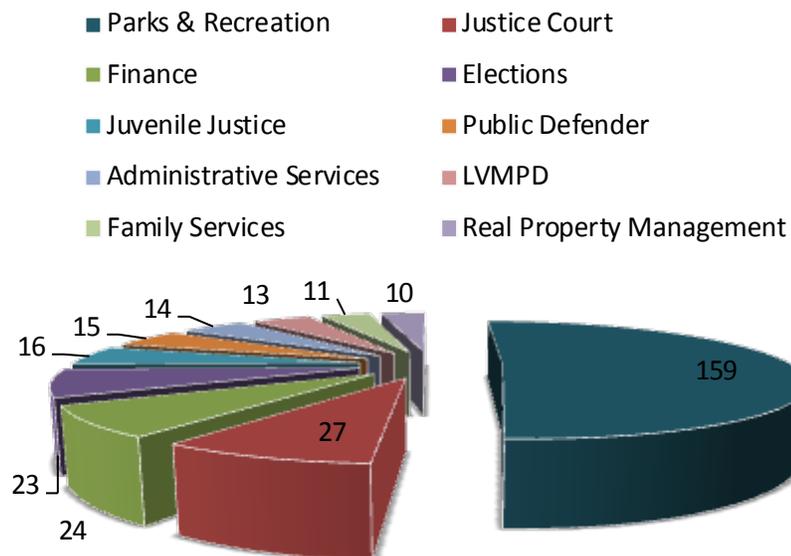
DETAILED RESULTS

Many Active Email Accounts Not Valid with Potential Network and Mainframe Access (HIGH)

We examined all email users within the domain of “ClarkCountyNV.gov”. We found that of 5,464 email users (excluding generic users), 379 (7%) are no longer employees and one test account existed.

We also reviewed five vendor accounts, and none had an expiration date. Vendor accounts are a risk, as the vendor may no longer be contractually affiliated with the County but still have ability to obtain or provide information/direction that can be confidential or damaging.

**Withdrawn Employees with Active EMail Accounts
by Department
(10 or More)**



It is apparent that current methods used to disable an account and established processes are not adequate to prevent and detect inappropriate access to email service or that email accounts are valid. It is the individual department’s responsibility to notify Information Technology to terminate network and

email services. Authorization forms through the Service Now application have been established for departments to easily notify Information Technology. However, Information Technology is not always notified when an email account is no longer valid due to employees withdrawing, transferring, or when an external user such as a vendor is no longer affiliated with the County. County Management has established formal guidelines regarding email use. Neither departments nor Information Technology are following these guidelines consistently. We believe it is the ultimate responsibility of Information Technology to assure that active email accounts and network access are valid through adequate security to prevent and detect threats.

The greatest risk associated with invalid active accounts is that County network access also potentially remains active, as does other access to County applications allowed through RACF, the Mainframe system. Significant applications reside on the County's mainframe system such as the Assessor application, District Attorney case management system, Social Service CACTUS system, jail system known as C-Track, Juvenile Justice system, and others. The risk that confidential information is inappropriately shared or County applications are inappropriately accessed is greatly increased when invalid active email accounts are used. Invalid active accounts also leave the County susceptible to threats and increases liability. Further, Information Technology is not in compliance with County Information Technology Directives that state user accounts must be disabled if they remain inactive for a period exceeding 60 days.

The risk is increased for the two departments (Air Quality Management and Development Services) that have distributed responsibility as opposed to a centralized responsibility residing with Information Technology. The risk is that these departments will grant network access without being monitored by Information Technology, placing network security at risk. We believe that Information Technology has a responsibility to monitor access provided by decentralized administrators to ensure overall security of the network and information systems resources.

Recommendation

1. Implement procedures to actively validate user accounts, including network access, on a consistent basis in compliance with County Information Technology Directives.

2. Realign responsibilities for notification to disable accounts. Such notification efforts should be coordinated between Human Resources, Purchasing, and Information Technology.
3. Provide a list of email users (internal and external users) to departments for validation on a periodic basis. Invalid accounts should be immediately disabled.
4. Implement procedures to monitor access provided by decentralized administrators.

**Inconsistent
Identification of
Internal and
External Users
(HIGH)**

Not all active accounts have sufficient information to determine whether it is valid. Of the 5,464 email accounts reviewed, 184 (3%) could not be matched to Clark County personnel data. Employees are assigned a personnel number when hired, but this information is not always available when an email account is activated. Further, departments do not provide a vendor number when requesting vendor email accounts. Obtaining this information would provide Information Technology with the means to validate email accounts. Information Technology has not made identifying information in the form of personnel numbers and vendor account numbers mandatory when requesting activation of an email account.

Of the five vendor email accounts examined, two could not be located within the County's financial vendor lists to determine County affiliation. The three vendors that could be identified did not have purchase order activity within the year, and may no longer have an affiliation with the County. We also found that one of the five vendors had two separate email accounts.

Without a process for validating information, it is possible for IT and departments with distributed responsibility to set up an email account and grant email and network access to virtually anyone.

Recommendation

1. Require departments to provide personnel and vendor numbers when requesting email accounts. If the personnel number is not available at that time, the department should provide the information once it is obtained.
2. Enter this information into user accounts in order to facilitate validation reviews of email accounts and granted network access.

3. For vendor accounts, include a County representative sponsor and contact number for any questions.

Emails Retained Indefinitely (HIGH)

Emails sent from and received by users in the ClarkCountyNV.gov domain are never permanently deleted. County Information Technology Directive Number 2, Email Policy, states that employees must maintain a copy of emails in a separate repository or print out and manually place records in a separate file. However, there is concern that policies may not be strictly followed and emails may have become the place of record. Information Technology does not have the tools necessary to sort through voluminous emails to identify record types for retention. As a result, emails continue to be retained indefinitely.

Storage for the email system is currently up to 14.4 terabytes of data. Replication of emails and backups is 132 terabytes and the archive and its replication is 22 terabytes. As each new email arrives or is sent, it is written to the active system, the archive, and is backed up for each of those locations. Therefore, each email can be stored in four locations at any one time, and two of those locations indefinitely (archive and archive backup). The fact that users are not limited in the amount of email they can have in their active mailbox causes a greater use of storage during replication. We were not able to develop a reasonable cost estimate for this method of storage.

The number of emails replicated and the need for more storage space continues to grow without any destruction of records. The voluminous number of emails is also problematic when record searches are done for management inquiries or during the discovery process of litigation. Providing security for large databases becomes more complex with the need to have many servers, data files, and multiple storage sites.

We believe that efforts to retain emails indefinitely will not be feasible in the future due to unforeseen and indeterminable events such as rising costs or workforce efforts to maintain voluminous information without corruption. The County also increases the risk of liability over confidential information being shared and historical information availability.

Recommendation

1. Establish policies specifying that email is not to be used as a repository for records and that email content that does qualify as a record is changed to some other format for retention.

2. Develop schedules for purging of e-mails in accordance with record retention policies.
3. Set reasonable mailbox size limits for users.
4. Provide a cost analysis of storage use and future needs for the exchange system in order for management to make appropriate decisions over data retention.

**“Send As” Names
No Longer Valid
(MEDIUM)**

The email system contains 145 users with “Send As” privileges. These users are able to send email as if it were being sent from another individual. Information Technology does not validate these privileges once email accounts are activated. However, employees may transfer or the responsibilities may change so that they should no longer have these privileges. These privileges are usually granted on behalf of upper level management, and those users may not realize that another employee is able to send email under their name. We found that seven users able to send as another employee were terminated employees, four users with individuals able to send messages on their behalf were no longer employed with the County, and three “Send As” names could not be verified based on the County’s personnel data.

The validity of County email communications may be compromised when “Send As” privileges are not closely monitored.

Recommendation

1. Validate “Send As” privileges with employees annually.

**Passwords Not
Required and
Never Expire
(MEDIUM)**

Email accounts for 85 users are set not to require a password. Further, email accounts for 34 users are set to have network passwords that never expire. During testing, we found that all accounts currently have a password set, even if not required. However, users with accounts that do not require passwords may set a password and then change to using no password. In that case, anyone with the user name may access any programs that do not require separate passwords and the email account of that user. The user name is usually the same as the email user name that is readily available through many resources. This places a risk for unauthorized users to access, change, and/or disseminate confidential information. Allowing users to never change passwords is not in accordance with County policies over network access security.

Recommendation

1. Change the setting on each of the accounts identified above to require a password that expires within the parameters required by Information Technology Directive 1.

Recovery of Exchange System Not Tested (LOW)

While Information Technology does have recovery procedures, the email system replication is not tested to determine whether replicated data is recoverable. Should a disaster or a significant disruption of service occur, Information Technology is not assured that the exchange system can be recovered fully and without data corruption. The exchange system is considered a critical component of the County, as it is vital for communication. Due to the number of backups to the active email system, we believe the risk based on this weakness is relatively low.

Recommendation

1. Test recovery of exchange system data.



Louis Carr, Jr., Chief Information Officer

Michael Lane, Deputy Chief Information Officer
Lester Lewis, Deputy Chief Information Officer

MEMORANDUM

To: Angela Darragh, Director Clark County Audit Department
From: Louis Carr, Jr., Chief Information Officer
Subject: Management Response to E-mail Audit
Date: April 30, 2014

The following information is presented in response to the Clark County Audit Department's e-mail audit conducted in October – December 2013.

Finding#1 - Many Active Email Accounts Not Valid with Potential Network and Mainframe Access

Concur. IT will use a report created by the Human Resources Department that lists each employee who was terminated, hired or transferred in/out of that department and IT will reconcile that report against our list of e-mail accounts. That process should be in place in August 2014.

Finding#2 - Inconsistent Identification of Internal and External Users

Concur. IT will modify our account creation process to request additional information from the department requesting the email account. We will also modify our process so that if all necessary information is not given up front, we will set that account to expire in 30 days. That process should be in place in August 2014.

Finding#3 - Emails Retained Indefinitely

Concur. IT will establish an email retention policy and develop schedules for purging of e-mails in accordance with record retention policies. It will also set reasonable mailbox size limits for users and provide a cost analysis of storage use and future needs. The email policy should be in place by October 2014. Other aspects of this finding will take months or even years to fully implement.

Finding#4 - Send As Names No Longer Valid

Concur. IT will report annually and notify users on whose accounts "Send As" or "Send on Behalf of" privileges are set. The departments will have the responsibility of responding to IT in a timely manner to validate that need still exists. This finding should be addressed no later than June 2014.

Finding# 5 - Passwords Not Required and Never Expire

Concur. IT will audit our e-mail accounts for non-expiring password. Users will be notified that the password policy is being enforced and be given adequate time to change software and/or business process. The impact of this finding may require departments to invest in updating their technology. In some cases, the cost of updating the system may be excessive and may require additional funding. This finding should be addressed no later than July 2014.

Finding# 6 - Recovery of Exchange System Not Tested

Concur. IT today has the ability to test a partial recovery of the Exchange system. Testing of entire Exchange environment will occur with implementation of disaster recovery for Clark County. This finding should be addressed no later than January 2015.