BERNALILLO COUNTY

NEW MEXICO

Information Technology

Internal Audit

December 2014

REDW LLC

CPAs | Business & Financial Advisors

REDW LLC
CPAs | Business & Financial Advisors

redw.com

Bernalillo County Internal Audit
Information Technology

Executive Summary

SUMMARY OF PROCEDURES

REDW performed an internal audit of the Bernalillo County Information Technology environment, general controls and security. Our consulting services were for the purpose of providing suggestions and recommendations to management to improve the efficiency, effectiveness, and security of the general information technology (IT) controls.

We performed a variety of procedures, including:

- Evaluating IT governance and oversight of the IT security program.
- Interviewing relevant IT personnel to gain an understanding of the IT environment.
- Obtaining and evaluating administrative instructions related to IT, other internal IT policies and procedures, and related documentation.
- Evaluating and testing security and logical access control processes including access to sensitive data and potential access by terminated employees.
- Assessing and testing access change management processes.
- Evaluating and testing security controls over workstations, mobile devices and removable media.
- Obtaining and evaluating the IT Disaster Recovery Plan (DRP) and assessing whether recovery of data and resources can be achieved in a timely manner.
- Obtaining and evaluating the computer security incident response plan (CSIRP).
- Obtaining and evaluating user acceptable use policies and agreements.
- Assessing system change management and configuration management processes.
- Evaluating IT security awareness training and testing employee security awareness.
- Evaluating data backup and restore policies and procedures.
- Assessing software inventory and license tracking processes.
- Performing a walkthrough of the data center to determine physical security and environmental controls.

SUMMARY OF OBSERVATIONS

There were many areas during the course of our testing, where we found controls were functioning properly and procedures were being followed. The County has a dedicated IT security group within the IT Department. They are responsible for, amongst other things, monitoring security controls and security audit logs. Many effective security controls were in place and physical security of the data center is good. Data is regularly backed up and stored off-site.

Significant high and moderate risk observations are presented below.

- ***IT Disaster Recovery Plan*—**The County does not have a formal, written IT disaster recovery plan or policy. There is no IT disaster recovery strategy other than recovery from backups. A business impact analysis (BIA) was performed several years ago to determine the criticality of data, applications and systems, and to determine recovery time objectives (RTO) and recovery point objectives (RPO) for systems and data. The BIA needs to be updated. Servers and data were being backed up nightly to removable media and the media was stored in a secure off-site facility for 90 days, which is what is required by County Legal. The County should develop and implement an IT DRP as soon as it is practically possible. A business impact analysis should be done as the first step of this process to identify critical applications, functions and processes and determine recovery time and point objectives.

- ***Removable Media Security*—**Administrative Instruction IT12 addresses controls over removable media. Removable media includes flash memory devices such as USB thumb drives, cameras, MP3 players, removable hard drives (including hard drive-based MP3 players), optical disks such as CD/DVD disks, and floppy disks. Of particular concern are USB thumb drives and other USB storage devices. These are considered by security experts and the Federal Bureau of Investigation (FBI) to be one of the greatest risks to network and data security. AI IT12 states that users are only allowed to use removable media purchased by the County IT Department. From interviews with IT personnel, they tell users that USB drives are prohibited. The County should consider implementing automated preventive controls over the use of USB flash drives. These automated controls can be configured to block the use of USB flash drives or automatically encrypt them if they are not encrypted.

- ***Security of Computers in the Human Resources (HR) Department*—**The County Human Resources Department has its own IT personnel who manage desktops, laptops and HR servers. As part of our workstation testing, we tested security controls on eight HR workstations. We found that some users were local administrators, two computers had not been updated with security patches in over five months, and Trend Micro antivirus application was out-of-date. Users should not be local administrators as this allows them to change security settings and download and install software. Security patches should be centrally managed.

- ***Local Administrator Rights*—**Administrative Instruction IT03 Acceptable Use of Information Systems states that only IT personnel are to be given local or global administrative rights. During our workstation testing, we determined that some users were local administrators on their workstations.

Being a local administrator allows the user to perform all administrative tasks on their computer including changing security settings and installing software. Management should ensure that users are not local administrators on their workstations unless there is a documented and approved business reason to grant them such access.

- ***IT Governance*—**The County does not have any formal structured IT governance process. Deputy County Managers meet weekly and all significant issues are discussed; however, this not an IT governance or steering committee that focuses on the IT needs of the organization and helps prioritize projects and resources.

- ***User Access Control Policies and Procedures*—**There is not a formal documented user access control policy. IT implemented a new Technology Request Form (TRF) and procedure in July 2014. This procedure is documented and addresses how users receive access to the network and applications, how access is changed, and how access is removed when they are no longer employed by the County.

  From interviews with IT personnel and the results of our test work it appears that the process for termination of user access does not always work as it is supposed to and IT is not always informed in a timely manner of users leaving employment. The County should develop a formal User Access Control Policy that addresses current practices and ensure that the user access termination procedures are communicated throughout the organization and enforced.

- ***Data Storage***—AI IT09 Desktop/Laptop Usage Guidelines requires that all sensitive or critical data is stored on network servers. From the results of our workstation testing it is apparent that some users store County data on their local desktops/laptops. Laptops are not encrypted. Loss of a laptops could result in sensitive data stored locally being lost or compromised. Users should receive training on the importance of storing County data on network drives. Laptop hard drives should be encrypted.

* * * * *

Further detail of our purpose, objectives, scope, procedures, and recommendations are included in the full internal audit report. In that report, management describes the corrective action being taken for each recommendation.

We received excellent cooperation and assistance from the various departments during the course of our interviews and testing. We sincerely appreciate the courtesy extended to our personnel.

REDW LLC

Albuquerque, New Mexico
March 26, 2015

Bernalillo County Internal Audit
Information Technology

Table of Contents

REDW LLC
CPAs | Business & Financial Advisors

redw.com

Bernalillo County Internal Audit
Information Technology

Report

INTRODUCTION

We performed the internal audit services described below solely to assist Bernalillo County in evaluating the Information Technology environment, general controls, and security. Our services were conducted in accordance with the Consulting Standards issued by the American Institute of Certified Public Accountants, Generally Accepted Government Auditing Standards, and the terms of our contract agreement for internal audit services. Since our procedures were applied to samples of transactions and processes, it is possible that significant issues related to the areas tested may not have been identified.

An entrance conference was held on December 8, 2014, at which time most items needed for the audit were requested and had been received. Fieldwork began on December 8, 2014. An exit conference was held on March 12, 2015, and final management responses were received on March 26, 2015.

Although we have included management’s responses in our report, we do not take responsibility for the sufficiency of these responses or the effective implementation of any corrective action.

PURPOSE AND OBJECTIVES

Our internal audit focused on evaluating the overall IT environment, general IT controls and security processes and establishing whether controls tested were adequate, effective and provided the appropriate levels of security.

SCOPE AND PROCEDURES PERFORMED

In order to gain an understanding of the IT infrastructure, policies and procedures, and security controls, we interviewed the following personnel:

- Paul Roybal, CIO
- Rod Rolston, Assistant CIO
- Kevin Smith, Infrastructure Manager
- Lawrence Chavez, Security Administrator

- Michael Gruen, IT Project Manager Systems
- Carolina Fernandez, Quality Assurance Manager
- Jessica Maestas, Application Manager
- Steven Gregg, Records Manager
- Felipe Rodriguez, Desktop Support Supervisor
- Rudy Elebario, Network Supervisor
- Victor Schexnayder, IT Project Manager MDC
- John Herrera, System Administrator

Background and Understanding

In order to understand the IT environment, IT governance, general IT controls and security controls we performed the following:

- Read and analyzed various IT related Administrative Instructions, internal IT policies and procedures and other related documentation.
- Read and assessed the draft IT Incident Response Plan.
- Gained an understanding of the following:
  - Data center access to assess physical security and environmental controls.
  - User access control process for setting up new users, change of position and termination of employment.
  - Backup and restore process.
  - Change management process.

Test Work

We performed the following test work:

User Logical Access Controls: The County implemented a new user access request form in July 2014. We obtained a list of all newly hired employees, employees who changed job position, and employees who left employment since July 2014. We selected 14 new hires, 9 position changes, 15 terminated employees and 15 IT personnel and tested the required documentation and approval process was completed:

- Before new hires were given access to the network and applications.
- For each employee that changed to a new position that required a change to the network and applications.
- For each employee leaving employment to determine that their access to the network and applications was removed in a timely manner.

Workstation Security: To verify the security of workstations, and determine if security controls had or could be changed, we performed the following on a sample of 29 workstations:

- Checked whether employees had administrator rights on their computer.

- Checked the date of the most recent Microsoft security patch/update and Trend Micro virus pattern update.
- Tried to disable and enable the Trend Micro Antivirus application with the employees logged in.
- Checked controls over password protected screen savers.
- Checked for business files in “My Documents” folder and on C: Drives.

Change Management Testing: The County implemented a formal change management program in March 2014. We judgmentally selected 15 system change requests out of a total of 242 change requests made since March 2014, and assessed whether the change management policy and procedures were followed. Specifically, we determined whether the change requests were approved, documented, prioritized, tested and whether the affected departments were informed in a timely manner of the changes and any anticipated downtime.

Tested the backup and restore process and off-site storage of backup media by performing the following:

- Determining whether the backup schedule was followed by reviewing the backup schedule and comparing information to the dates on the backup tapes on-site and off-site.
- Reviewed two daily backup status reports automatically generate by Data Protector software.
- Performed a walkthrough of the data center to assess physical and environmental controls.

Tested system maintenance tracking to test the following:

- Verify that maintenance is being performed on Tier 1 systems.
- Test the timing of updates.
- Test proper notification of updates performed.

Performed inquiries to determine if an IT Disaster Recovery Plan was in place and whether:

- The plan is complete and up-to-date.
- A business impact analysis has been done.
- The plan has been tested and employees trained.
- The plan includes realistic recovery time objectives and recovery point objectives.

Obtained and assessed the computer security incident response plan to determine whether:

- The plan is complete and up-to-date.
- The plan is adequate for responding to a cybersecurity incident.
- The plan has been tested and employees trained.

Evaluated IT security awareness training and tested employee security awareness by performing the following:

- Evaluated the IT security awareness PowerPoint presentation.

- Assessed employee security awareness as part of the workstation testing process.

Observations, Recommendation and Management Response

We identified the following exceptions and provided recommendations related to the County's IT infrastructure, policies and procedures and other security controls and processes:

1) IT Disaster Recovery Plan

The County does not have a formal, documented IT disaster recovery plan (DRP) and there is no real IT disaster recovery strategy in place. An alternate disaster recovery site has not been identified. A business impact analysis was conducted several years ago to determine criticality of data, applications and systems, and to determine recovery time objectives (RTO) and recovery point objectives (RPO) for systems and data. This has not been updated.

The backup schedule is complex and varies depending on the department and application. From interviews with IT personnel it appears that backups are retained for 90 days as required by the County Legal Department. The recovery plan has not been formalized or tested, although in the event of a disaster, restoration could be performed by restoring data from the off-site nightly backups.

Potential Risk: High—Lack of a formal and tested IT disaster recovery plan could result in the County being unable to recover its data and systems in a timely manner in the event of a disaster or other IT emergency.

Recommendations

1. Develop and implement a formal DRP policy.
2. Develop an IT disaster recovery strategy and implement an IT disaster recovery plan (DRP) as soon as is practically possible. The business impact analysis should be reviewed and updated as the first step of this process to identify any changes to critical applications, functions and processes, recovery time and point objectives. The DRP should address formal testing of the plan and training for personnel. Testing and training should be conducted at least annually.
3. Develop formal written data backup and restore policy and procedures based on current practices. Ensure that the policy addresses legal requirements.

Management's Response

The County wide business impact analysis will be reviewed and updated where necessary and used to formulate the DRP policy by September 30, 2015. IT will develop and implement a formal DRP policy pending budget availability by December 31, 2015. A new backup system is being deployed and once completed, IT will develop written data backup and restore procedures by June 30, 2015.

2) Removable Media Security

AI IT12 addresses controls over removable media. Removable media includes flash memory devices such as USB thumb drives, cameras, MP3 players, removable hard drives (including hard drive-based MP3 players), optical disks such as CD/DVD disks, and floppy disks. Of particular concern are USB thumb drives and other USB storage devices. AI IT12 states that users are only allowed to use removable media purchased by the County IT Department. AI IT12 also requires that if sensitive information is stored on removable media it must be encrypted. However, this is not being done.

AI IT03 prohibits plugging in nonCounty owned computer equipment into the County information systems. From interviews with IT personnel they tell users that USB drives are prohibited. From interviews with employees and observation, personally owned USB devices are plugged into the County information systems.

Potential Risk: High—Removable media is considered by security experts and the FBI to be one of the greatest risks to network and data security. A great deal of data can be stored on USB drives and they are by default are not secure. USB drives are also becoming a source of malware infection.

Recommendations

1. Perform a risk assessment to determine the level of risk removable media presents to the County. Depending on the results of the risk assessment consider implementing automated preventive controls over the use of USB flash drives. These automated controls can be configured to block the use of USB flash drives or automatically encrypt them if they are not encrypted.
2. Allow only authorized personnel to use County owned USB drives for business purposes and ensure that these are encrypted.

Management's Response

Any removable media device plugged into our client systems today is scanned by Trend Micro OfficeScan. If virus or malware is detected it is cleaned or quarantined by Trend. The use of USB ports in today's computer environment is unavoidable. IT Security will conduct a risk assessment by June 30, 2015 to document the risk removable media presents to the County. Appropriate IT staff have been briefed on the requirements of AI IT12. IT will continue to work with users to find alternative solutions to using USB thumb drives; however, if no other option exists we will issue a clean USB device. IT Security will add information to AI IT12 that defines "sensitive information" for staff.

3) Security of Computers in the Human Resources (HR) Department

The County HR Department has its own IT personnel who manage desktops, laptops and HR servers. Although HR has its own IT personnel the computers are all on the same network but on a different domain as the rest of the County. As part of our workstation testing we tested security controls on eight HR workstations. We found the following security concerns:

- On three workstations the user was a local administrator. This allows them to change security configurations and to download and install software.
- Two computers had not been updated with Microsoft security updates in over five months. HR computers were configured to do their own automatic updates and were not centrally managed. This configuration can be changed by the user.
- Several workstations had versions of Trend Micro antivirus software that were out-of-date and no longer supported by Trend Micro.

Potential Risk: High—Lack of operating system security updates could result in security breaches, malware infections and data corruption could affect not just the HR Department but all areas of the County.

Recommendations

1. For security and efficiency reasons, management should consider bringing the HR IT area into the main IT area.
2. Ensure that users are not local administrators on their workstations.
3. Ensure that Microsoft patches/updates are centrally managed. Regular scans/reviews should be done to monitor all updates.

Management's Response

We will have an IT consultant conduct a technology assessment of IT services within the County to provide recommendations for improved operational effectiveness, reliability, and security of existing systems. This is estimated to be completed by the end of fiscal year 2015. Authorization for local administrator rights were in place on two desktops due to a camera system software upgrade. This designation was only for the period of time that the software was installed and tested and was removed promptly thereafter. Approval was given by the HR Director. The vendor and the HRIS team worked together on this upgrade. The employees whose boxes were affected by the upgrade had no role in the software installation and did not know that "local administrator" was in play. The third desktop had local administrator designation for a printer install under the previous domain name of Personnel which has been replaced by a new domain—HR Domain. No security configurations were changed and no software was downloaded or installed this desktop. The HR Domain has an Active Directory Group Policy that forces each desktop PC to automatically download and install windows updates on a daily basis at 3 AM. Local administrators do not have the ability to change configurations for Windows updates. HRIS and the Security Administrator for the IT Department are working to ensure that HR is linked to the System Center, thus addressing central management. The IT Department pushes out the virus signature updates for all desktops in the county, including the HR Department. The HRIS Manager and the Security Administrator recently verified that all desktops in the HR Department have the current version.

4) Local Administrator Rights

Administrative Instruction IT03 states that only IT personnel are to be given local or global administrative rights. During our workstation testing we determined that the users were local administrators on 29% of the workstations tested.

Being a local administrator allows the user to perform all administrative tasks on their computer including changing security settings and installing software. Four of the 29 workstations tested had nonwork related and prohibited software installed, which creates a security risk to the County.

Potential Risk: High—Users with local administrative rights can download and install software on their local machine. This can result in malware infections, licensing issues, and software corruption from incompatible applications. In addition users with administrative rights are able to change security controls configured on their computers.

Recommendations

Ensure that users are not local administrators on their workstations unless there is a documented and approved business reason to grant them such access.

Management's Response

IT has created a script that identifies users in the workstation administrator group. The script has been run and users have been removed from the administrator group. IT Security will run the script weekly and remove unauthorized users from the workstation administrator group. IT Security will maintain a list of authorized exceptions.

5) IT Governance

The IT Governance Institute (ITGI) defines IT governance as:

"The governance of IT is the responsibility of executives, and board of directors, and consists of the leadership, organizational structure and processes that ensure that the enterprise's IT sustains and extends the organization's strategies and objectives."

The County does not have any formal structured IT governance process. The IT Department is large and has a good internal structure and reporting process. There is not a formal structure for communications between the organizational areas/departments and IT. Deputy County Managers meet weekly and all significant issues are discussed; however, this not an IT governance or steering committee that focuses on the IT needs of the organization and helps prioritize projects and resources.

Potential Risk: Moderate—Lack of formal IT governance can result in a disconnect between IT goals and the goals of the organization and result in heightened risk exposure. IT projects may not be prioritized correctly or resources are not available to complete projects. Effective IT governance enables IT to be responsive to business needs.

Recommendations

1. The County should consider creating a formal IT Governance or Steering Committee comprising of members of the organization's management as well as IT. The committee should meet regularly (quarterly to start, then semi-annually once established). The committee should not address the day-to-day running of IT. It should not be chaired or run by IT but by someone else in the organization. The committee should be formalized with a charter and meetings should have formal agendas and be documented through minutes.

Management's Response

IT will chair a committee to create a formal IT Governance process. The process will include creating an IT Governance committee that meets regularly and follows a structured process that focuses on IT needs of the County and IT project prioritization. The formal written IT Governance process will be submitted for approval by the County Executive staff by December 31, 2015.

6) User Access Control Policies and Procedures

There is not a formal documented user access control policy. IT implemented a new Technology Request Form (TRF) and procedure in July 2014. This procedure is documented and addresses how users receive access to the network and applications, how access is changed, and how access is removed when they are no longer employed by the County.

From interviews with IT personnel and the results of our test work it appears that the process for termination of user access does not always work as it is supposed to and IT is not always informed in a timely manner of users leaving employment. Human Resources sends a bi-weekly list of terminated employees to IT. In addition, the IT Security Group monitors active directory for user accounts that have been idle for 90 days or more and automatically disables them. However, we found one active account out of 15 accounts tested for a terminated employee. The terminated employee's account had been active for five months after the employee's termination date.

Once the TRF is completed it is stored on SharePoint as documentation of access and approval. The naming convention for the completed forms does not relate to the user or the date of access creation/change. This makes it difficult to find the correct form.

Potential Risk: Moderate—Failure to disable network and application accounts of users who have left the County can potentially result in the user (or other users) accessing the network and data they are no longer authorized to access. This risk is increased if the user has remote access to the network.

Recommendations

1. The County should develop a formal User Access Control Policy that addresses current practices.
2. Ensure that the user access termination policy and procedures are communicated throughout the organization and enforced.
3. Ensure that user accounts are randomly selected and reviewed as required by AI IT06. If this is not feasible consider doing an annual review of user access levels to the network, applications, and data, and update the AI to reflect this requirement.
4. Consider changing the naming convention of the completed TRF to make them easier to find and review.

Management's Response

IT will add a requirement to the Administrative Instructions to address how a user requests access to technology resources by June 30, 2015. IT will review the termination process with the goal of automating the process by September 30, 2015. IT will remove the requirement in AI IT06 concerning the random review of user accounts and focus on a monthly review of domain and administrator accounts by June 30, 2015. IT will review how the TRF form is stored and named to determine if there is a simpler method.

7) Data Storage

AI IT09 requires that all sensitive or critical data is stored on network servers. The AI informs users that County desktops and laptops are not backed up by IT.

From the results of our workstation testing it is apparent that some users store County data on their local desktops/laptops. Ten of the 29 workstations tested had County data stored on the local hard drive. Users have access to network drives but some users do not understand the difference between local hard drive and network drives.

Laptops are not encrypted and therefore the loss of a laptop could result in sensitive data being compromised.

In addition from interviews with Records Management it appears that some sensitive data is stored on share drives where it can be accessed by any user.

Potential Risk: Moderate—Storing data, particularly sensitive data, on the local hard drive of a computer could result in potential data breach or loss of important data that is not backed up.

Recommendations

1. Communicate to users, through security reminders and/or as part of security awareness training, the difference between local storage and network storage. Emphasize the importance of storing all County data on network drives and in correct folders on network drives.
2. If there is enough storage and backup space, consider redirecting My Documents from the local hard drives to a network drive.
3. Strongly consider encrypting the hard drives on all County laptops.
4. Review users access permissions on folders on the network containing sensitive data or that are likely to contain sensitive data.

Management's Response

IT will add information to the security training at employee orientation specifically addressing storing data on network drives by May 30, 3015. IT will work with HR to create a computer training module in their Leaving Management System (LMS) scheduled for deployment later this year. This module will include security awareness training and network storage.

8) Software License Tracking

Hardware inventory is done annually and all new hardware is entered into an inventory spreadsheet. Similar inventories are not done for software and software license tracking. IT does not have an automated system that scans all computers on the network for software inventory and license tracking. The County has an enterprise license agreement with Microsoft and this covers licenses for all Microsoft software. Similar license agreements are not in place for other software products. A process for software asset management is important in an organization as large as the County and helps with redistribution of licenses and management of legal risk associated with software ownership and license agreement violations.

Potential Risk: Low—Failure to track and monitor software licenses could result in license violations and monetary fines. Also, failure to track and monitor software licenses can result in unnecessary software purchases.

Recommendations

1. Develop, document and implement a software asset management program. The goal of the program should include:

- Reducing software and support costs by negotiating volume contract agreements and eliminating or reallocating underutilized software licenses.
- Enforcing compliance with County policies and standards.
- Improving productivity by deploying the right kinds of technology more quickly and reliably.

2. Consider investing in an automated software inventory tool that intelligently “discovers” software installed across the network and collects software file information such as title, product ID, size, date, path, version, and license number.
3. Consider centralizing the purchase of desktop software to the IT Department.

Management’s Response

IT will research automated software inventory tools and make a recommendation for purchase subject to budget availability to County management by May 30, 3015. IT will also include a software management piece within the IT Governance project. The Software management piece will be a future phase to be completed in FY 17.

9) IT Security Awareness Training

County employees receive security awareness training as part of new hire orientation. We obtained and assessed the security awareness training power point developed by the IT Security Group. This presentation covers most aspects of security awareness. The IT Security Group sends out alerts and security reminders to all employees. The County employees do not receive regular/annual security awareness training after new hire orientation. Additionally, there are no policies and procedures to address security awareness training and frequency of training.

Potential Risk: Low—Lack of security awareness training for employees can result in security breaches, data loss, and malware infections. The fact that the IT Security Group sends out security reminders and alerts to all employees makes this risk slightly lower than it would be normally.

Recommendations

1. Develop and implement IT security awareness training policy and procedures.
2. Provide an IT security awareness training refresher course every couple years to remind employees of their continuing responsibilities for security, and require mandatory attendance for all employees.
3. Ensure that the County security policies and information on social engineering are included in the training.
4. Track and monitor employee security awareness training to ensure all employees attend.

Management’s Response

IT will work with HR to create a computer training module in their new LMS system scheduled for deployment later this year. This module would make it mandatory for all County employees the complete the security awareness training module annually. Social Engineering attacks are already included in the employee orientation training and would be included in the new security training module.

10) Computer Security Incident Response Plan (CSIRP)

IT has developed a draft computer security incident response plan. It addresses roles and responsibilities, escalation procedures, six stages of response, and emergency contacts.

However, it lacks the following elements of a complete plan:

- How and to whom employees report potential incidents.
- A section requiring regular testing of the plan and how this will be done (table top exercises, scenario walk-throughs, etc.).
- A section requiring training of team members on the plan.

Potential Risk: Low—Lack of a complete CSIRP could result in the organization failing to respond and contain an information security incident. The County has dedicated IT security personnel and the incident response plan is in the process of being developed.

Recommendations

Computer security incidents, malware attacks, as well as data breaches, can and do happen. Having appropriate pre-defined processes in place assists an organization more effectively respond to, investigate, and mitigate the impact of incidents. This is considered a security best-practice in accordance with National Institute of Standards and Technology Special Publication 800-61.

1. Complete and implement the incident response plan. The plan should include the missing elements listed above.
2. As soon as possible after the plan is complete the plan should be tested and CSIRP team members should receive training.

Management's Response

IT has completed the Incident Response Plan. This plan will be submitted to county management for final approval. The plan specifically identifies who security incidents are reported to and who is responsible for management of security incidents. IT will test the final approved incident response plan by 30 Jul 2015.

11) Password Settings

Authentication is the process of identifying an individual, usually based on a username and password. The use of a unique user ID and password is considered single factor authentication and is not considered a strong form of authentication unless the passwords are long, complex and changed frequently.

Passwords are required to be a minimum of eight characters with complexity enforced which is considered a security best-practice.

Users are required to change their password every 180 days. Security best-practice recommends passwords to be changed at a minimum of every 90 days.

Potential Risk: Low—Failure to change passwords regularly could potentially allow a password to be cracked by a hacker or other unauthorized person.

Recommendations

Consider requiring users to change their passwords at least every 90 days.

Management's Response

IT agrees that changing passwords every 90 days is an ideal situation. However, in a large environment users do forget their passwords and have multiple passwords to remember. Requiring users to change passwords more frequently causes additional security risks such as users forgetting their passwords requiring more password reset requests, writing their passwords down, using the same password across multiple accounts, etc. We believe our 180-day requirement is the optimal compromise between ideal security and creating additional security risks to the County's network. As discussed above, IT does require password complexity which helps to mitigate the risk of 180-day password changes.

12) Password Resets

One of the frequent support calls to the Service Desk is for password resets from users who have forgotten their passwords and/or have locked their accounts. The Service Desk does not have a procedure to verify that the user is who they say they are. This is a potential security risk.

Potential Risk: Low—Lack of verifying a user is who they say they are could result in someone else changing a user's password and getting unauthorized or inappropriate access to the network and data. This risk is low because all support calls are documented in the Track-It system and active directory keeps a log of password changes and resets.

Recommendations

Develop and implement a procedure to verify the identity of a user calling the Service Desk for a password reset. This procedure could be improved, for example:

- A call back to their office phone number.
- Requesting their employee ID number.
- Requiring the user to answer a previously set up security question.

Management's Response

IT will develop and implement a procedure to verify users requesting a password reset by May 30, 3015.

13) Administrative Instructions

We obtained and assessed 19 Administrative Instructions (AI) that were IT related. Sixteen of the 19 have a review date of November 17, 2011. From interviews with IT personnel and other employees, observation, and the results of test work it appears the some AIs and current practices are not aligned. Examples include but may not be limited to:

- AI IT06 states that user accounts will be randomly selected and assessed for validity and access – this is not being done.
- AI IT03 requires any County nonpublic or confidential data stored on a laptop, mobile wireless device or tablet must be saved to an encrypted file system using approved software. This is not being done and there is no approved software.

Potential Risk: Low—Administrative Instructions provide the policies and controls that let users know what is acceptable or not acceptable to do with the County information systems. Failure to implement or enforce documented controls may result in the users ignoring or circumventing requirements. Failure to document requirements means that users may not know what is required of them.

Recommendations

Ensure that all AIs are reviewed and updated to reflect current practices or changed as needed to comply with AIs.

Management's Response

IT will review all IT Administrative Instructions and make changes to reflect current practices as required by September 30, 2015.

* * * * *

This report is intended for the information and use of the County management, the Audit Committee, members of the board of commissioners of Bernalillo County and others within the organization. However, this report is a matter of public record, and once accepted its distribution is not limited.

REDW LLC

Albuquerque, New Mexico
March 26, 2015