Neil Kelly
Clerk of the Circuit and County Courts
Lake County, Florida

Audit of BCC Web Server/Application Security

Internal Audit Division
Audit Report

Bob Melton, CPA, CIA, CFE, CIG
Director of Internal Audit

Audit Conducted by:
Jacqueline Holder, CISA, CISM, CRISC

Report No. BCC-112
December 20, 2013

Internal Audit Division
Phone (352) 253-1664
Fax (352) 253-1645

Clerk of the Circuit Court

Post Office Box 7800
Tavares, Florida 32778-7800

December 20, 2013

Board of County Commissioners

We have conducted our audit of the Web Server and Application Security function of the Board of County Commissioners' Communications Division, as requested by management and scheduled per the Clerk's Annual Audit Plan.

We appreciate the cooperation and assistance provided by the Communications Division, Information Technology Division, and other entities contacted during the course of our audit.

Respectfully Submitted,

Bob Melton
Bob Melton
Director of Internal Audit

CC: Honorable Neil Kelly, Clerk of Circuit & County Courts
David Heath, County Manager
Kelly LaFollette, Director of Communications

TABLE OF CONTENTS

INTRODUCTION

Scope and Methodology

We conducted an audit of the Web Servers and Application Security function of the Lake County Board of County Commissioners' Communications Division, as scheduled per our Annual Audit Plan. Our audit objectives were:

1. To determine if the County is in compliance with applicable laws and regulations.
2. To determine if processes for online payments and newsletter sign-ups are efficient.
3. To determine the adequacy of controls and the appropriateness of the level of authority regarding web site changes.
4. To determine the adequacy of social networking practices.

To determine if the County is in compliance with applicable laws and regulations, we researched payment card data standards, and reviewed County policies and procedures.

To determine if processes for online payments and newsletter sign-ups are efficient, we conducted tests using sample card data and entered various payment transactions using the County's online resources.

To determine the adequacy of controls and the appropriateness of the level of authority regarding web site changes, we reviewed change management processes.

To determine the adequacy of social networking practices, we reviewed applicable County policies and procedures, scanned existing County social networking sites for content and searched for unauthorized sites.

Our audit included such tests of records and other auditing procedures, as we considered necessary in the circumstances. The audit period was May 1, 2013 through June 30, 2013. However, transactions, processes, and situations reviewed were not limited by the audit period.

Overall Conclusion

We conclude that the County is in compliance with applicable laws and regulations. We conclude that processes for online payments and newsletter sign-up are efficient. We conclude that the adequacy of controls and the appropriateness of the level of authority regarding web site changes are inadequate.

We conclude that social networking policies and procedures should be enhanced and enforced, and all social networking sites should be monitored for unauthorized used. Opportunities for Improvement are included in this report.

Background

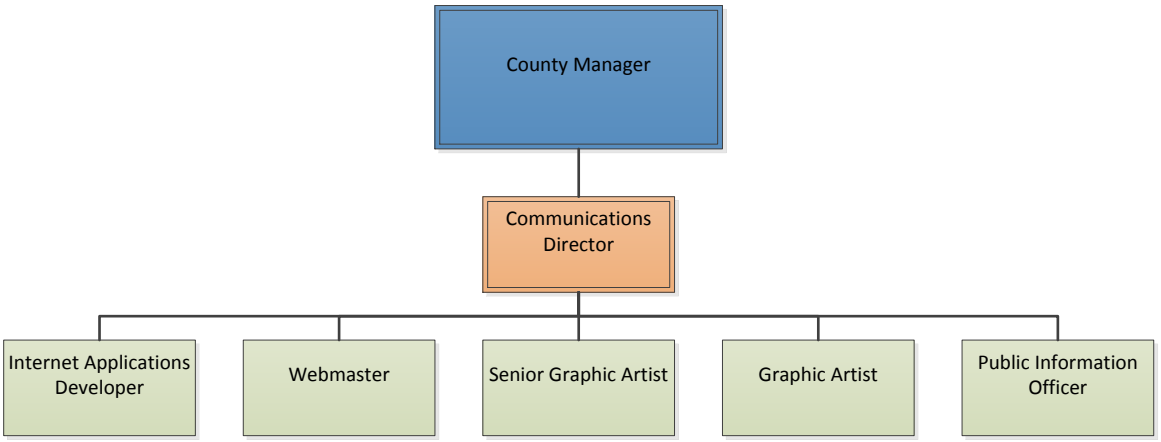
The Communications Department assists the departments within the Lake County Board of County Commissioners in expanding internal and external communications. This is accomplished through three key areas: web and multimedia development, graphic design, and media relations. The staff, which consists of one Public Information Coordinator, two graphic artists and two web developers, works as a team similar to an advertising agency, using the creative skills of all its members to produce ingenious solutions to a variety of communication-based projects.

According to management, one of the many duties assigned to the division involves working closely with the Department of Tourism and Business Relations to prepare advertisements and marketing materials to promote Lake County as a tourist destination. With funding provided through Lake County's tourist development tax, some of the recent projects completed for the department include the quarterly Special Events Guide, the 52-page Vacation Guide, Lake County's VIP Vacation Card materials and the Clermont Chain of Lakes Map.

The office also currently hosts and maintains several County agency Web sites, some of which include:
- Lake County Board of County Commissioners
- Lake County Property Appraiser's Office
- Lake County Supervisor of Elections
- Lake-Sumter Metropolitan Planning Organization (MPO)
- LakeXpress (the County's fixed bus route system)
- Lake County Library System
- Lake County Economic Growth and Redevelopment

From preparing the State of the County presentation and annual report, to helping inform the public of life-safety issues during times of disasters, the Communications Department strives to provide a consistent and timely message to the citizens of Lake County.

The organizational chart for the Communications Division is as follows:



The County utilizes the following social networking sites for which the Communications Division has responsibility for setting up and overseeing:

Twitter:

- Lake County Government
- Lake County Tourism
- Lake County Economic Development
- Lake County Library System
- Energy Efficiency Conservation Block Grant (EECBG) – (No longer being used.)
- LakeXpress

Facebook:

- Lake County Government
- Lake County Tourism
- Lake County Library System
- Economic Development
- Lake County Teen Court

Lake County Parks & Trails

- eNewsletters:
  - Lake County News Releases
  - Lake County Tourism
  - Lake County Government
  - Lake County Parks & Trails
  - Lake County Library System

Blog

- Lake County Florida's Blog

YouTube

- Lake County FL

OPPORTUNITIES FOR IMPROVEMENT

Our audit disclosed certain policies, procedures and practices that could be improved. Our audit was neither designed nor intended to be a detailed study of every relevant system, procedure or transaction. Accordingly, the Opportunities for Improvement presented in this report may not be all-inclusive of areas where improvement may be needed.

1. Policies and Procedures to Address the Maintenance of Servers and Firewalls Should Be Established.

During our review of the County's processes for maintaining the security over servers and firewalls, we found that there are documented Information Technology Department procedures for maintaining servers and workstations, but not for firewalls. We noted that the Communications Division has procedures for their division and their web servers. Procedures are necessary for providing instruction on how and when servers and firewalls should be maintained. Without proper procedures to ensure the continued maintenance over servers and firewalls, hackers can gain complete access to sensitive data, perform various attacks, and exploit software bugs, among other things.

The National Institute of Standards and Technology (NIST) has issued Special Publication 800-123 "Guide to General Server Security" to provide organizations with best practices for ensuring the proper maintenance and security of their servers and firewalls.

Section 4.1 of the Guide states:

> "Once an OS is installed, applying needed patches or upgrades to correct for known vulnerabilities is essential. Any known vulnerabilities an OS has should be corrected before using it to host a server or otherwise exposing it to untrusted users. To adequately detect and correct these vulnerabilities, server administrators should do the following:
>
> - Create, document, and implement a patching process.
> - Identify vulnerabilities and applicable patches.
> - Mitigate vulnerabilities temporarily if needed and if feasible (until patches are available, tested, and installed).
> - Install permanent fixes (patches, upgrades, etc.)"

We Recommend management institute policies and procedures for ensuring the maintenance and security of the County's servers and firewalls.

Management Response: We concur.

2. Vulnerability and Penetration Tests Should Be Conducted.

During our review of the County's procedures for ensuring all systems are secure from hacker attacks, we noted that the County Information Technology Department is not conducting vulnerability or penetration tests against their network, although they do have a package that provides extra protection against hacker attacks. By not conducting these tests, unidentified weaknesses can breach the security of the organization. Vulnerability and penetration tests are valuable tools that can benefit any security program, and they are both integral components of the process to identify weaknesses in an organization's infrastructure. A successful vulnerability test can provide an organization with the appropriate mitigation procedures required to either eliminate those weaknesses or reduce them to an acceptable level of risk. A penetration test takes the vulnerability assessment to the next level and attempts to exploit the vulnerabilities identified.

We Recommend management perform a vulnerability assessment regularly to identify and remediate known vulnerabilities. Penetration tests should be performed at least annually and after significant changes in the information systems environment.

Management Response: We partially concur. We will explore our options as this may have a fiscal impact.

3. Event Logs Should Be Monitored.

During our review of the County's system security, we noted that the County Information Technology Department is not monitoring system event logs. Routine log reviews and analysis are beneficial for identifying security incidents, policy violations, fraudulent activity, and operational problems shortly after they have occurred, and for providing information useful for resolving such problems. Logs can also be useful for performing auditing and forensic analysis, supporting the organization's internal investigations, establishing baselines, and identifying operational trends and long-term problems. The most important benefits to logging these events are increased security, increased awareness of network infrastructure problems, increased server, services, and application availability, fast detection of network outages and protocol failures, and fast detection of failed processes, services and batch jobs.

The National Institute of Standards and Technology (NIST) has issued Special Publication 800-92 "Guide to Computer Security Log Management" to provide organizations with best practices for setting up and monitoring system event logs.

Section 2.2 of the Guide states:

> "Log management can benefit an organization in many ways. It helps to ensure that computer security records are stored in sufficient detail for an appropriate period of time. Routine log reviews and analysis are beneficial for identifying security incidents, policy violations, fraudulent activity, and operational problems shortly after they have occurred, and for providing information useful for resolving such problems. Logs can also be useful for performing auditing and forensic analysis, supporting the organization's internal investigations, establishing baselines, and identifying operational trends and long-term problems."

We Recommend management institute procedures to review and monitor event logs on a regular basis, at least weekly, and enable triggers to notify appropriate personnel of suspicious activity.

Management Response: We partially concur. We will explore our options as this may have a fiscal impact.

4. Procedures for Deactivating Terminated Employees Should Be Enhanced.

While reviewing recent employee terminations, we noted the concerns below:

A. The deactivated date is not being entered in the employee's "Description" field in Active Directory.

   Lake County Procedure IS201, Active Directory, states that the date on which the employee was deactivated in Active Directory should be entered into the Description field.

B. Procedure IS201, Active Directory, does not specify the definition of timeliness for deactivating employees in Active Directory. Employees should be deactivated immediately upon termination of employment.

C. Terminated employees were found active in Active Directory after their termination date. Management was unable to provide sufficient documentation to justify the reason for employees still being active in Active Directory long after their termination date.

By not deactivating employees on a timely basis, the County is at risk of unauthorized access or malicious activities.

We Recommend management begin entering the employee's deactivated date in the Description field in Active Directory and maintain a paper trail of all employee terminations and justifications for delays in deactivation. Additionally, management should update procedures to require immediate deactivation of employees in Active Directory when completing their last working day.

Management Response: We concur.

5. Proof of Compliance With Credit Card Data Security Rules Should Be Provided.

The County has not provided proof of being PCI-DSS (Payment Card Industry-Data Security Standard) compliant. The County's third party credit card processor requires all of their merchants to be PCI-DSS compliant and provide proof of such by completing and submitting a self-assessment questionnaire (SAQ) and an Attestation of Compliance (AOC). The processor retains the right to charge non-compliant merchants a fee of $25 per month (effective July 30, 2010). This fee will be applied monthly until the merchant validates their compliance with the PCI DSS. In addition, the processor may also choose to terminate the merchant's agreement if they fail to comply with PCI DSS.

In order to determine compliance, we downloaded and completed the application self-assessment questionnaire. After the review, we determined that the County is PCI-DSS compliant. However, this self-assessment should be completed by management.

We Recommend management complete the required Self-Assessment Questionnaire and Attestation of Compliance.

Management Response: We concur.

6. Procedures for Change Management and Segregation of Duties Should Be Established.

During our review of the processes for applying changes to the various County web sites and social networking sites, we noted that there are no procedures in place for effective change management and segregation of duties. Although only authorized people are making web site and social networking site changes, those changes are not being reviewed and approved by a supervisor prior to being published to the live sites nor is segregation of duties being used for coding, testing and

uploading those changes. The Web Server Updates procedures describe which servers should be updated and how often. In addition, we noted the following:

A. Change logs are vague in that their descriptions are not detailed enough to convey the substance of the change.

B. The Web Server Updates procedure is not dated as to when it was created or last updated, and does not specify the use of a test server for testing changes or system patches prior to installation on the live servers (even though this is being done in practice).

Change Management can ensure standardized methods, processes and procedures are used for all changes, facilitate efficient and prompt handling of all changes, and maintain the proper balance between the need for change and the potential detrimental impact of changes. Segregation of duties is the concept of having more than one person required to complete a task as an internal control intended to prevent fraud and error. In essence, it is a level of checks and balances upon the activities of individuals.

Without effective change management procedures in place, the potential exists for unauthorized changes to be made to the County's web sites and social networking sites, and errors could go undetected for an undetermined amount of time.

We Recommend management establish procedures to address change management of web site and social networking site changes and include segregation of duties and documentation of changes.

Management Response: We partially concur. We will explore our options as this may have a fiscal impact.

7. Social Network Access of Employees Terminating Employment Should Be Deactivated on a Timely Basis.

During our review, we noted that some employees are not being deactivated from social network access on a timely basis. Although we noted no recently terminated employees having social networking access, several instances were noted in the past where social network access was not terminated for several days after termination of the employee. While a policy has now been established which requires timely termination of access, it is important that access actually be terminated immediately upon the employee's last work day.

Since the County does not exercise control over persons who are no longer employed, risk is increased that a former employee could take an inappropriate or malicious action using their social networking

account. Therefore, this period of access following termination of employment should be eliminated or minimized.

We Recommend management remove social networking account access immediately upon termination of employment.

Management Response: We concur.

8. The Use of Surrogate Social Networking Sites Should Be Prohibited.

During our audit of Lake County Animal Services, we noted that County staff were using a citizen surrogate to operate a Facebook page that was not approved by County management. An Animal Services employee would direct the information to be posted to the page and provide pictures of animals. In addition, monetary pledges were solicited on the page with instructions to contact the Animal Services employee with the amount of the pledge. The Animal Services employee subsequently provided information to the surrogate identifying the total pledges that had been received for each animal. Rescue organizations would then consider taking the animals knowing how much money they would receive for doing so.

Lake County Procedure LC-50, Section III states: "All requests for creation of any social networking accounts must be made to the Department of Information Technology, Information Outreach Division. Departments must complete and submit an application using the Social Networking Request Form…" This policy does not specifically address the use of surrogate social networking or provide for disciplinary action regarding employees who perform this activity.

The use of a surrogate has circumvented Lake County policy, and, therefore, eliminates the normal controls that the policy includes. The possibility of inappropriate use or postings is increased.

We Recommend County policy strictly prohibit the use of surrogate social networking and provide for appropriate action for any County employee performing such activities.

Management Response: We concur.

9. Adequate Social Networking Policies Should Be Established and Followed.

While reviewing the County's policies and procedures and the associated social networking sites, we found several concerns noted below:

A. The County social networking procedure (LC-50) and the related training guide have not been updated for more than three years. We noted the current procedure refers to MySpace, which is no longer used, and both documents refer to the Communications Division by its prior name of Information Outreach. Policies should be updated on a periodic basis to ensure all

information is current. By not having current information, users may be confused as to information contained in the procedure.

B. No policy restricts employees from commenting or posting on social networking sites, for official purposes, using their personal social networking accounts. Social networking policies or procedures should prohibit the use of personal social networking accounts for County purposes. We noted one instance where a County employee responded to a citizen's comment on the County's Teen Court Facebook page using her personal Facebook account. We noted another instance in which a County employee posted on Twitter using her personal name instead of the County departmental name. These practices could not only be misleading to the readers, but could also put a County employee in a risk position by disclosing their personal name and information.

C. Some social networking pages do not contain a disclaimer that is required by County policy. We noted that the County's blog site and the Lake County Library System Facebook page did not contain the disclaimer. After we notified management of this situation, disclaimers were added to the sites we identified.

Lake County Policy LC-50 states:

> "Each social media account must have the following public records notice clearly stated on the landing page of the social networking Web page: "Public comments made on this page are not considered official communications with Lake County Government, and will not be responded to. To contact Lake County Government, send your questions or comments to webmaster@lakecountyfl.gov. All content on this page is subject to Florida Public Records Laws."

By not including the required disclaimer, citizens may not understand the communication is public record and that comments or questions will not be answered.

D. The Lake County Florida Parks & Trails Facebook page was not blocking public posts on the main page. Procedure LC-50 states that all Facebook pages should be setup to block posts from the public on the main page. As a result, pages could contain content that dilutes the message provided by the County. It should be noted that management corrected this situation upon notification.

E. Some staff requesting social networking access have not signed the required training guide consent form. As a result, their social networking access is unduly delayed. The training guide consent form requires employees to represent that they have read the guide and understand its contents.

F. During our review, we noted provisions in the policy of another County that are not contained in Lake County's policy. These provisions should be considered:

a. Contributor shall not publish anything (on social networking sites) that may be construed as inappropriate (such as obscene or libelous material) while acting in their official capacity as a Contributor.

b. County departments should restrict the "Find People" and "Follow People" options. Department Directors are discouraged from "following" private citizens or commercial profiles from within their government social networking profile. While the County cannot stop all people from being "Friends", "Fans" or "Following Us", County Departments should not click onto the profiles of our "Friends", "Fans" and "Followers" without receiving approval from the County Manager.

c. County Departments should refrain from participating in dialogue and online discussions with social profile visitors.

d. Criteria regarding Accessibility Rights and the Sunshine Law.

e. Limit quantity of Tweets so as not to become a public annoyance.

f. There shall not be any links from the County Website to personal Twitter sites.

g. County Department employees are encouraged not to represent themselves as members of the Lake County Government workforce on social networking sites regarding matters specific to their official duties.

h. County Department employees shall not disclose any confidential or proprietary information of the County on any personal web application.

Social networking is a rapidly changing environment which provides many opportunities for abuse or misuse. Therefore, it is crucial that related policies be updated frequently to ensure all risks are reasonably controlled.

We Recommend management:

A. Update the procedure and training guide, review it on a periodic basis, and update further as needed.

B. Restrict employees from commenting or posting on social networking sites, for official purposes, using their personal social networking accounts.

C. Ensure the required disclaimer is contained on all applicable social networking pages.

D. Ensure public posts to social networking pages are blocked where appropriate.

E. Ensure the training guide consent form is signed on a timely basis.

F. Consider adding the noted additional provisions to the County's social networking procedure.

Management Response:

A. We concur.
B. We concur.
C. We concur.
D. We concur.
E. We concur.
F. We concur.