Performance Audit of the San Diego Convention Center's Information Technology Infrastructure

JULY 2012

Audit Report

Office of the City Auditor

City of San Diego

This Page Intentionally Left Blank

THE CITY OF SAN DIEGO

July 19, 2012

Carol Wallace, President and Chief Executive Officer
San Diego Convention Center

Transmitted herewith is an audit report on the San Diego Convention Center's IT Infrastructure. We have completed this report as requested by the Convention Center. This report is presented in accordance with City Charter Section 39.2. Management's response to the report is presented on page 8.

We would like to thank the Convention Center's staff for their assistance and cooperation during this audit. All of their valuable time and efforts spent providing us information is greatly appreciated. The audit staff responsible for this audit report are Stephen Gomez, Toufic Tabshouri, and Chris Constantin.

Respectfully submitted,

Eduardo Luna
City Auditor

cc: City of San Diego Audit Committee Members

This Page Intentionally Left Blank

Table of Contents

This Page Intentionally Left Blank

Introduction

The City Auditor's Office (OCA) conducted a performance audit of the San Diego Convention Center's (SDCC) information technology network infrastructure. We performed this audit at the request of SDCC and in accordance with the terms of a Service Level Agreement with SDCC.

This audit was the first of four potential audits identified by a high-level risk assessment that we had previously performed for SDCC. The purpose of this audit was to evaluate some of the primary risk areas in SDCC's information technology (IT) environment. Those risk areas are:

1. IT infrastructure operations and security;
2. The financial system;
3. The outsourced human resources system contract; and
4. The management of IT system implementations; specifically, the implementation of the customer relationship management system.

Objectives, Scope, and Methodology

Our main audit objective was to identify security and operational risks to SDCC's IT infrastructure. We performed a risk assessment of SDCC's IT environment, including a high-level review of the main applications, operating systems, and network infrastructure. We performed a more detailed assessment SDCC's infrastructure security and operations. We reviewed SDCC's IT infrastructure as of June 14, 2012.

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.

Audit Results

SDCC Has Reduced Internal IT Risks Through Outsourcing

Our audit did not have any significant findings, but we noted several opportunities for improving IT controls and enhancing IT security. We evaluated existing IT practices at SDCC against established professional guidelines for IT management.[1] The main reason why we did not find any significant issues is that SDCC has pursued a strategy of outsourcing its high-risk IT functions, including its human resources system and the IT maintenance and support for its financial system. While SDCC has lowered its "in-house" risks through outsourcing, we identified some minor issues that SDCC management should address to further improve network security regarding IT documentation, segregation of duties, and network activity logs.

SDCC Has Limited Governing Documentation for Information Technology

We noted several opportunities for creating or improving existing IT documentation. Documentation of policies is important for several reasons. The first is that documentation serves to preserve institutional knowledge, which is crucial in the event of employee turnover. The second reason is that policy review and approval by management educates management on information technology issues and provides them an opportunity to shape the policies. Lastly, having formal policies facilitates the enforcement of good security practices across the organization.

Security Policy

The Information Systems Department (IS Department) has created a security policy, but this policy is not dated and has not been formally approved by SDCC management. Professional guidance on IT policies recommends that policies be approved by management and dated. Dating policies is important in order to facilitate tracking effective policy dates, changes, and revisions. Furthermore a review of the record of changes provides insight into the frequency at which policies are being

[1] Most of our audit criteria were derived from *Control Objectives for Information and Related Technologies* (COBIT), which is a framework for IT governance and management published by the Information Systems Audit and Control Association (ISACA).

updated to meet the changing needs of an organization. This is particularly important in information technology, where change is constant.

Security Strategy

SDCC does not have a documented security strategy. Professional guidance recommends the creation of a security strategy to insure that threats to information have been identified, that risks have been evaluated, and that the organization has either accepted these risks or taken measures to prevent or mitigate them.

Key Daily Operations

For the same reasons of knowledge management mentioned earlier, all required tasks pertaining to the daily IT operations of SDCC should be documented. Examples of these tasks include the activities of the network engineer, such as monitoring network traffic, ensuring backup runs are performed, updating and patching servers and desktops, reviewing network logs, and trending issues and problems to identify common causes.

Server States

Although SDCC servers are now virtualized,[2] the information technology function should still provide documentation on the state of key servers such as the ones that operate the financial system and store nightly backups. Such information includes a listing of all the software that is installed on the server, special or specific configuration settings, and the services (such as programs that run in the background) that run on it. Server state documentation entails an "allow list" showing which services are permitted to run and which are run. This documentation is important to enable verification that a server is configured correctly and not running unauthorized programs.

Additional Segregation of Information Technology Functions Can Enhance Controls

Segregation of duties is an important control principle that reduces the likelihood that a single employee can hijack critical processes and make changes without approval or detection. Small IS Departments normally find it difficult to implement checks by segregating high-risk employee duties, because they do not have not enough employees to share the work. The SDCC IS Department employs one senior network engineer who

[2] Virtualization is a trend in information technology management that utilizes software to present the appearance of discrete pieces of hardware to computer users. In reality, there is no separate physical hardware component. Virtualization is popular because it reduces hardware purchase costs facilitates management of various IT processes.

supervises two junior staffers, all of whom have the same level of access to SDCC systems. The Department has taken steps to mitigate risk by outsourcing critical functions such as IT support for SDCC's financial system.

However, the Department should take additional measures and implement compensating controls and alerts. For example, backup of network activity is currently performed by the network engineer. To improve controls, periodic testing and restoration of the backups should be performed by one of the junior employees to ensure the backup systems work. The IS Department should document all critical processes such as backup, server updates, security monitoring, and then attempt to assign responsibility for each process to more than one employee. Full segregation of duties is not a realistic goal, since employees in small departments are cross trained and need access to perform the duties of other employees who are on leave or otherwise unavailable. In such cases, however, critical or high risk activities should be logged in a secure location and reviewed by the IS Director on a regular basis.

Network Activity Logs Operate At Default Settings

The logging of network activity at SDCC has been left at default server settings, and the retention period for logs is at the default setting as well. Professional guidance indicates that logging should be tailored to environmental risks in order to capture important events and minimize the amount of data that is logged. Minimizing logged data is important because large log files are difficult to review and consequently less likely to be reviewed. Logging activities can be further divided into security and troubleshooting logs, based on the particular activity or event. Examples of events that should be logged are remote access logins (especially outside normal business hours) and logins to the financial system. The logs should include enough information to be useful for security analysis, containing information such as the user who logged in, systems accessed, and core activities while accessing these systems. In addition, log files should be stored in a restricted location. Where possible, Segregation of Duties should be enforced for the access to the logs, where the IT personnel responsible for performing certain high risk activities should not monitor that activity or have the ability to modify the logs. At this time, all IT

employees have access to the activity logs, which are stored locally and appear to be geared more for troubleshooting than for security.

In addition to establishing the optimal logging activity for SDCC, the logs should be reviewed on a regular basis and the appropriate monitoring reports should be created. If a log is not monitored or used, it should not be activated as it is only consuming resources without a benefit. Monitoring activities is an important element of network security to insure that high-risk events are reviewed by the appropriate IT personnel.

Conclusion

We would like to thank SDCC and the IS Department staff for their help on this audit; we could not have conducted our audit in such a short timeframe without their assistance. Our suggestions for improvement involve documenting current practices and enhancing certain control and monitoring activities. Implementing those suggestions will improve the security of network operations, and bring SDCC practices in line with professional guidelines. We look forward to working with you in the future.

Management's Comments

The San Diego Convention Center Corporation's management would like to thank the City Auditors for their thorough audit of our information systems technology infrastructure. We are certainly pleased that the audit did not have any significant findings.

Based on the auditor's recommendations, the Information Systems (IS) department will take to opportunity to make enhancements in the following areas.

- Information Technology documentation for the security policy, security strategy, and daily operations will be enhanced in order to preserve institutional knowledge. Regarding server state, since Microsoft Windows Server 2008 R2 is based on least access roles. We only install the role or roles necessary for an application or service to operate correctly and we currently separate applications by assigning them to a unique virtual server. We have created a server and application list which will be used as a baseline. We can then compare any new services or applications to the baseline and ensure that any changes are identifiable.
- Additional Segregation of Information Technology Functions has been achieved due to a recent staffing change that allowed the IS department to segregate the information technology functions.
- Network Activity Logs Operating at Default Settings: The network activity logs produced by the Microsoft 2008 R2 operating system although set at its default level are appropriate for the high level of post event activity that the IS department has deemed necessary in order to investigate server issues. The logs will continue to be monitored on a daily basis by the network engineer and all critical or high risk activities will continue to be reviewed by the IS Director.

Again thank you and we look forward to working with you again in the future.