Internal Audit

2016 Data Centers Assessment Internal Audit Report

Approved: Isaac S. Clarke
Isaac S. Clarke

May 13, 2016
Report Reference: R-16-3

Contains sensitive security information that should not be publicized pursuant to Utah Code 63G-2-106 and 63G-2-305(12). Such information is also controlled under 49 CFR parts 15 and 1520 and may not be released without appropriate authorization. This information is highlighted in yellow in the internal version of the Report and should be redacted from any public version of this Report.

Executive Summary

Background and Procedures Performed

Information Technology (IT) is embedded into everything the Utah Transit Authority (UTA) does. The use of IT results in electronic data that must be secured in such a manner as to ensure the data's confidentiality, integrity and availability. IT security enables ongoing operations and is needed to comply with regulatory requirements. A data center is a critical component of IT security. UTA moved its data center from its Meadowbrook facility to the University of Utah's downtown data center in January of 2016 to expand services and improve the organization's IT security and availability.

An internal audit was performed to assess the design and operational effectiveness of controls at UTA's new data center and other locations where critical IT equipment and data reside to safeguard the Authority's assets and maintain their availability to support business operations. The period of the audit was from January 1, 2016, to March 21, 2016. The primary areas of focus include:

- Physical Security
- Environmental Control
- Backup and Recovery
- Data Center Administration

Procedures performed on each process in this review included inquiries of functional management and personnel to understand the business processes and control framework, review of process and procedural documentation, inspection of facilities, and inspection of management documentation to determine whether the identified controls have been implemented and are functioning as intended.

Key Management Issues

UTA does not have a disaster recovery site for its data center. Backup records are currently replicated to a telecom closet at another site near the data center that lacks adequate physical security and environmental controls. The IT department began the process of identifying and securing a disaster recovery site in 2015 and expects to have a disaster recovery site in place in the latter part of 2016.

Telecom closets do not have adequate physical security and environmental controls. Access to telecom closets is not restricted only to personnel with responsibilities that require the access. Environmental controls are not consistently administered. Telecom closets should be reviewed and categorized by the importance and sensitivity of the IT assets each closets holds. Access rights and current environmental controls for each telecom closet should be reviewed and approved by IT to ensure physical security and environmental controls align with its respective categorization. The processes for provisioning and reviewing access to the data center and telecom closets should be modified to ensure the appropriateness of access to all IT critical facilities and the timely removal of access when necessary.

Overall Process Conclusion

Except for the backup and recovery controls and access provisioning, controls for the data center are designed and operating effectively.

Controls for telecom closets were not designed and operating effectively.

Intentionally Left Blank

Table of Contents of Protected Information

Findings and Recommendations

1. *UTA should have a disaster recovery site for its data center.* An organization should have a disaster recovery site in place that can be used, in the case that the data center goes down, to recover backups and restore critical systems and data. Requisite hardware, connectivity, and the storage of backup files should align with the organizational disaster recovery plan. A disaster recovery site should also be located far enough away from the data center to limit its exposure to the same risks that comprise the data center's operations.

   Failure to have a disaster recovery site may result in UTA losing data and computer systems, shutting down of operations for longer than necessary, higher costs to obtain a site at the time of an emergency, and reputation damage.

   Audit procedures found that UTA does not currently have a disaster recovery site. However, it was also noted that IT identified the need for a disaster recovery site in 2015, began the process to identify an appropriate site and provider, and accounted for the additional expense in its 2016 budget. IT was in the process of writing a request for proposal and waiting for the 2015 carry-over capital budget at the time of this audit.

   Recommendation R-16-3.1: *The Deputy Chief – Information Systems Manager should secure or set-up a disaster recovery site that is sufficiently removed from the data center that it will not be impacted by the same events that might render the primary location inoperable.*

2. *UTA should ensure that telecom closets have adequate environmental controls.* It is important to maintain a suitable environment within telecom closets for IT equipment to function under normal conditions. Additional controls should be in place to protect IT hardware and support its operation during abnormal events (e.g., loss of power, power surge, fire, etc.). Not all telecom closets are created equal in that some may house more critical or sensitive hardware than others. Consequently, the nature and extent of environmental controls needed for a telecom closet may vary. Organizations should have clear guidelines of what circumstances would require certain environmental controls.

   Failure to have appropriate environmental controls in place may result in hardware damage, system failure, loss of data, and financial and reputational damage.

   Audit procedures found that two (2) of the five (5) telecom closets inspected lacked adequate environmental controls. [redacted]

   Recommendation R-16-3.2: *The Deputy Chief – Information Systems Manager should assess telecom closets to identify those housing hardware that require environmental controls and implement those controls as needed.*

3. *Access to UTA's data center and telecom closets should be restricted to personnel with job responsibilities requiring access.* Entry points to facilities housing critical IT resources (IT facilities) should be secured to prevent unauthorized access. Additionally, a formal process should be in place for provisioning access to IT facilities. The process should require that:

   - Requests for access to IT facilities are approved by a designated IT approver.
   - IT periodically reviews individuals with access to IT facilities.
   - Access is removed from individuals who no longer require access in timely manner.
   - All approvals, reviews and terminations of access to IT facilities are documented.

   Unauthorized access to the data center or telecom closets may result in hardware theft or damage and unauthorized access to or loss of data.

   [redacted]

   [redacted]

   Recommendation R-16-3.3: *The Chief Safety and Security Officer should work with IT and Facilities to ensure that telecom closets are adequately secured.*

   Recommendation R-16-3.4: *The Deputy Chief – Information Systems Manager should work with Facilities to formalize the process for provisioning access to the data center and telecom closets to ensure that IT reviews and approves access requests.*

   Recommendation R-16-3.5: *The Deputy Chief – Information Systems Manager should establish a formal process for reviewing individuals' access to the data center and critical telecom closets to ensure that access is limited to only personnel whose responsibilities require that they have access to these facilities.*

Management Action Plans

The following are the planned actions that UTA Management has drafted in response to the findings and recommendations proposed by Internal Audit in the preceding section.

Recommendation ID	Mgt. Agreement	Owner (Name and Title)	Target Completion Date
R-16-3.1	Yes	Deputy Chief – Information Systems Manager	August 31, 2016
Recommendation:	*The Deputy Chief – Information Systems Manager should secure or set-up a disaster recovery site that is sufficiently removed from the data center that it will not be impacted by the same events that might render the primary location inoperable.*		
Action Plan:	The Deputy Chief – Information Systems Manager will continue the current procurement process to identify and contract with a third party to provide a suitable disaster recovery site for UTA by the end of August 2016.		

Recommendation ID	Mgt. Agreement	Owner (Name and Title)	Target Completion Date
R-16-3.2	Yes	Deputy Chief – Information Systems Manager	July 31, 2016
Recommendation:	*The Deputy Chief – Information Systems Manager should assess telecom closets to identify those housing hardware that require environmental controls and implement those controls as needed.*		
Action Plan:	The Deputy Chief – Information Systems Manager will conduct a telecom closet assessment to identify environmental control needs and will oversee the implementation of the necessary controls. [redacted] [redacted]		

Recommendation ID	Mgt. Agreement	Owner (Name and Title)	Target Completion Date
R-16-3.3	Yes	Chief Safety and Security Officer	September 30, 2016
Recommendation:	*The Chief Safety and Security Officer should work with IT and Facilities to ensure that telecom closets are adequately secured.*		
Action Plan:	The Chief Safety and Security Officer will work with IT and Facilities to ensure that telecom closets are adequately secured.		

Recommendation ID	Mgt. Agreement	Owner (Name and Title)	Target Completion Date
R-16-3.4	Yes	Deputy Chief – Information Systems Manager	August 31, 2016
Recommendation:	*The Deputy Chief – Information Systems Manager should work with Facilities to formalize the processes for provisioning access to the data center and telecom closets to ensure that IT reviews and approves access requests.*		
Action Plan (1):	The Deputy Chief – Information Systems Manager will formalize the internal process for granting and removing personnel's access to the data center to ensure that only appropriate individuals are granted access [redacted]		
Action Plan (2):	The Deputy Chief – Information Systems Manager will work [redacted] to also control granting or removing access for employees needing access to the telecom closets. This will include [redacted] to review and approve requests for access to the telecom closets.		

Recommendation ID	Mgt. Agreement	Owner (Name and Title)	Target Completion Date
R-16-3.5	Yes	Deputy Chief – Information Systems Manager	September 30, 2016
Recommendation:	*The Deputy Chief – Information Systems Manager should establish a formal process for reviewing individuals' access to the data center and critical telecom closets to ensure that access is limited to only personnel whose responsibilities require that they have access to these facilities.*		
Action Plan:	The Deputy Chief – Information Systems Manager will establish a process [redacted]		

Report Distribution

This report is to be distributed directly to the following individuals.

- Interim General Manager/President/CEO
- Chief Technology Officer
- Deputy Chief – Information Systems Manager
- Chief of Staff and Chief Safety and Security Officer
- Facilities Maintenance Manager

Appreciation is expressed to management for their cooperation in supporting this internal audit.

Audit Team Members

Auditors assigned to this project were Brian Ledbetter and Riana De Villiers.