THE UNIVERSITY OF TEXAS-PAN AMERICAN
OFFICE OF AUDITS & CONSULTING SERVICES

PHYSICAL SECURITY

Report No. 13-11
April 2, 2013

Dr. Robert S. Nelsen, President  
The University of Texas-Pan American  
1201 W. University Drive  
Edinburg, TX  78539

Dear Dr. Nelsen,

As part of our fiscal year 2013 Audit Plan, we completed a risk based audit of Physical Security. The objective of this audit was to determine whether the physical security measures for information technology resources were effective and operating as intended. The scope of the audit included all facilities that house centralized information technology resources.

We performed audit procedures that included interviewing employees, obtained activity logs for room access, and employee assignment information. Additionally, we tested security measures for a sample of rooms with information technology resources.

We concluded that the security measures taken to protect physical security were effective and operating as intended. Critical computing and networking equipment were kept behind locked doors, were not accessible to unauthorized persons, and were protected by video surveillance systems and electronic door locks. Although, several physical security measures were successfully deployed, we recommended some improvements to enhance physical security of the University’s information technology resources.

We appreciate the courtesy and cooperation received from management and staff during our audit.

Sincerely,

Eloy R. Alaniz, Jr., CPA, CIA, CISA  
Executive Director of Audits, Compliance & Consulting Services
Table of Contents

**EXECUTIVE SUMMARY**  .................................................. 1

**BACKGROUND**  ..................................................... 2

**AUDIT OBJECTIVE**  .................................................. 2

**AUDIT SCOPE AND METHODOLOGY**  ................................. 2

**AUDIT RESULTS**  .................................................... 3

**CONCLUSION**  .......................................................... 7
The major processes performed at The University of Texas – Pan American (UTPA) rely heavily on information technology resources. The majority of these processes require the storage of personal and sensitive information. The University is required to properly manage the security of information technology resources. Appropriate physical security controls are essential to manage and protect the University’s information technology resources. Proper management of physical security is a State requirement under the Texas Administrative Code (TAC) Rule 202.73 - Managing Physical Security. This rule states that “the institution of higher education head or his or her designated representative(s) shall document and manage physical access to mission critical information resources facilities to ensure the protection of information resources from unlawful or unauthorized access, use, modification or destruction.”

The objective of this audit was to determine whether the physical security measures for information technology resources were effective and operating as intended. The scope of the audit included all facilities that house centralized information technology resources.

We concluded that the physical security measures taken to protect physical security were effective and operating as intended. Critical computing and networking equipment were kept behind locked doors, were not accessible to unauthorized persons, and were protected by video surveillance systems and electronic door locks. Although several physical security measures were successfully deployed, we observed the following:

**Inappropriate Access**
- Three employees and one student who had left the University still had access to rooms with key computing and networking equipment. The employees did not go through the exit process and did not return their key fobs. The employees’ fobs had not been used. We did not verify if the student’s fob had been used.

- Two key fobs were assigned to employees that had job roles that did not require access to rooms with computing and networking equipment. These fobs had not been used.

**Monitoring**
- The University Locksmith was not providing IT management with a list of employees with key fob access to rooms that house computing and networking equipment, and IT management was not regularly requesting this list.

- The University Locksmith was not providing IT management with activity logs for rooms that house computing and networking equipment, and IT management was not regularly requesting these logs.
BACKGROUND

Information resources are essential to daily operations of the University. UTPA’s information resources include the student system, Banner, the financial and human resource system, Oracle E-Business, and many other systems that support operating processes. In order to provide key processes, these systems must store personal and sensitive information. Therefore, it is essential that the University protect its information resources both logically and physically. The Division of Information Technology is responsible for the physical security of information technology resources. The University Locksmith is responsible for issuing key fobs to employees and generating activity logs for rooms that house computing and networking equipment.

The University has three buildings that house key information technology resources. In addition, there are many rooms throughout campus that contain network equipment.

Managing physical security is a State requirement under the Texas Administrative Code (TAC) Rule 202.73 - Managing Physical Security. The University manages physical security by using several security measures for rooms with computing and networking equipment. These measures include electronic door locks, rooms located in restricted areas, preventing access to unauthorized persons, and using video surveillance systems.

AUDIT OBJECTIVE

The objective of the audit was to determine whether the physical security measures for information technology resources were effective and operating as intended.

AUDIT SCOPE & METHODOLOGY

To accomplish the audit objective, we interviewed employees, obtained activity logs and employee assignment information. The scope of the audit included all facilities that house centralized information technology resources. Additionally, we tested a sample of rooms with information technology resources.

Our audit was conducted in accordance with guidelines set forth in The University of Texas System’s Policy 129 and The Institute of Internal Auditor’s International Standards for the Professional Practice of Internal Auditing. The audit was conducted between the months of October 2012 through February 2013.
AUDIT RESULTS

Key Fobs (fobs)

Fobs are security tokens with built-in authentication used to open electronic door locks. Most rooms that house computing and networking equipment are protected with electronic door locks and are maintained by the University Locksmith. They provide several benefits over conventional door locks as follow:
- Fobs are difficult to duplicate,
- Fobs access can be immediately removed if lost or stolen,
- Do not require rekeying,
- Cannot be picked,
- Log date and time of entry, and
- Provide long term cost savings.

Electronic locks assist the University in the management of physical security and are essential for compliance with TAC 202.73 - Managing Physical Security.

Our test sample included the two main data rooms, the media storage facility, a room that houses a personal computer (PC) cluster supercomputer, and eight rooms with networking equipment. We obtained a list of employees with fobs to those rooms from the University Locksmith. This list indicated that there were 168 key fobs, and the list was compared to a report of active employee assignments.

We determined that this list of employees with fobs to rooms that house computing and networking equipment was not generated by the Locksmith regularly nor was it requested by IT management. We also determined that IT management did not have a master list of employees with access to their facilities. Additionally, IT management does not review the list of employees with active fobs and request removal of access from employees who have left the University or whose job roles do not require the access.

Below is the status of the 168 key fobs:

<table>
<thead>
<tr>
<th>Total Fobs</th>
<th>Fob Status</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Ex-employees</td>
<td>Not returned to the University Locksmith</td>
</tr>
<tr>
<td>1</td>
<td>Ex-employee</td>
<td>Returned to the University Locksmith</td>
</tr>
<tr>
<td>1</td>
<td>Ex-student</td>
<td>Not returned to the University Locksmith</td>
</tr>
<tr>
<td>1</td>
<td>Employee from Distance Education</td>
<td>Employee’s job role does not require access to room with computing equipment.</td>
</tr>
<tr>
<td>1</td>
<td>Employee from Facilities Management</td>
<td>Employee’s job role does not require access to rooms with networking equipment.</td>
</tr>
<tr>
<td>2</td>
<td>Custodial Services</td>
<td>Fobs lent out to custodial personnel as needed</td>
</tr>
<tr>
<td>Total Fobs</td>
<td>Fob Status</td>
<td>Comments</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>7</td>
<td>Physical Plant</td>
<td>Fobs lent out to maintenance personnel as needed</td>
</tr>
<tr>
<td>25</td>
<td>Police Department</td>
<td>Some fobs were issued to the police chief and others were assigned to the Police Dept.’s Key Track system.</td>
</tr>
<tr>
<td>20</td>
<td>University Locksmith</td>
<td>Fobs kept in the University Locksmith work room and were pre-programmed and ready to be issued to new users when needed.</td>
</tr>
<tr>
<td>107</td>
<td>IT, Physical Plant, Police Department, and Environmental Health and Safety</td>
<td>Employees from these four areas had access to the main data rooms and to rooms with key networking equipment.</td>
</tr>
<tr>
<td>168</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Recommendations:**

1. The Executive Director for IT Services should immediately request that the access be removed for those ex-employees and the student who did not turn in their fobs as well as the employees whose job duties did not require this access.

2. The Director of Facility Management should develop an annual process to provide IT management with a list of employees with access to rooms that house computing and networking equipment.

3. The Executive Director for IT Services should maintain a master list of employees with access to facilities with computing and networking equipment. In addition, IT management should review the list of employees with active fobs and request removal of access from employees who have left the University or whose job roles do not require the access. Completion of this process should be done annually and signed off by IT management.

**Management’s Responses:**

1. Meeting is scheduled with locksmith on April 3, 2013 to discuss scope of work for work order. Items to be discussed include:
   - Update list of personnel with access to rooms
   - Update list of communication rooms and critical rooms
   - Process for IT staff to receive annual list of personnel with access to network and mechanical rooms and critical rooms on an annual basis.

Work order requesting removal of non-essential personnel from access lists will be submitted by April 12, 2013. Final implementation is to be completed by August 30, 2013, if locksmith’s schedule permits.

Implementation Date: **August 30, 2013**.
2. An initial report will be issued on or before close of business April 15, 2013. This report will test data content and format to meet the needs of IT management. Adjustments to the data would follow as recommended. Thereafter, an annual report would be issued to IT management on the Monday of the first week in August, in this case Monday August 5, 2013.

Implementation Date: **August 5, 2013**

3. Meeting is scheduled with locksmith on April 3, 2013 to discuss list of employees with access to communication rooms and to mechanical rooms. Work order requesting removal of non-essential personnel from access lists will be submitted by April 12, 2013. On April 3, 2013 we will have the list of personnel that should have access to each location (critical rooms, communication rooms, mechanical rooms), but reconfiguration of locks will not be fully implemented until August 30, 2013, if locksmith’s schedule permits.

Implementation Date: **August 30, 2013**

**Logs for Electronic Door Locks**

One of the advantages of electronic door locks is that they have the capability of generating logs of people who use their fobs to enter rooms fitted with these locks. The process to acquire the data to generate these logs requires the University Locksmith to physically connect an interface to the electronic door lock and upload the activity data to a hand-held device. This data is then loaded to a desktop computer that hosts a key and fob management software called Schlage. After the data is loaded, the Locksmith can generate an activity log. Activity logs have the name of the employee whose fob was used to enter the room and also includes the date and time of entry.

Reviewing these logs can help identify inappropriate activity. Inappropriate activity may include, but is not limited to, activity after or before normal operating hours, activity during weekends, activity from employees who are no longer with the University, and excessive activity from employees from departments that do not have IT job responsibilities (ex: Facilities Maintenance, Facilities Operations Support, etc.). Regular monitoring of activity logs is essential to properly manage physical security.

We obtained a list of employees with fobs to the rooms tested and activity logs for some of the rooms from the University Locksmith. The Locksmith only provided activity logs for the two data rooms and the media storage facility. The Locksmith could not provide the activity logs for the room that houses the PC cluster supercomputer and the eight rooms with networking equipment. He indicated that he did not have time to generate the reports. Therefore, we reduced our test sample of rooms. Our test of activity logs included the comparison of activity logs and the list of employees with fobs to the rooms. We determined that no inappropriate entries were identified. Individuals entering these rooms were authorized to access these rooms and the time
of access was appropriate. We determined that the activity logs were not regularly generated by the Locksmith. Additionally, they were not requested or reviewed by IT management on a regular basis. Therefore, no monitoring was taking place.

**Recommendations:**

4. The Director of Facilities Management should develop a quarterly process to provide IT management with activity logs for rooms that house computing and networking equipment.

5. The Executive Director for IT Services should develop a process to review activity logs for rooms that house computing and networking equipment. This process should be performed every quarter and completion of this process should be signed off by IT management.

**Management’s Responses:**

4. We are currently working on standardizing a document/spreadsheet that exhibits access activity for communication rooms. We intend to submit a draft copy of the audit trail to IT Management on June 4, 2013 for review. Once the content and format have been agreed upon, we can begin a routine cycle of audit trails for quarterly review.

   Implementation Date: June 4, 2013

5. Meeting is scheduled with locksmith on April 3, 2013 to discuss scope of work for work order. Items to be discussed include:
   - List of personnel with access to rooms
   - List of critical rooms, communication rooms, and mechanical rooms
   - Process to provide IT staff logs on a quarterly basis
   - Process for IT staff to download logs to review on a quarterly and as needed basis.
   Work order, if required, will be submitted by April 12, 2013. Modifications to software may require support from software vendor. Final implementation is to be completed by August 30, 2013, if locksmith’s schedule permits.

   Implementation Date: August 30, 2013

**Testing of Physical Security**

Aside from electronic door locks, the University deploys additional measures which contribute to the management of physical security. The rooms in our test sample included these additional security measures as follow:
The University of Texas – Pan American
Physical Security
Risk Based Audit

- Were locked when visited,
- Had locks and doors in good working condition,
- Did not have unauthorized persons present when visited, and
- Did not have any apparent security weaknesses that could be exploited.

We observed that the two main data rooms, the media storage facility, the room that houses the PC cluster supercomputer, and the rooms that house key networking equipment have video surveillance systems that were monitored by IT personnel. These video surveillance systems provide a variety of features. These features include continuous video feeds of rooms being monitored and emails with pictures when motion is detected. The data rooms have both features. The media storage facility, the PC cluster supercomputer room, and key networking rooms only have systems that email pictures when motion is detected.

We concluded that these features greatly enhance our physical security for our critical systems.

CONCLUSION

The security measures taken to protect physical security were effective and operating as intended. Critical computing and networking equipment were kept behind locked doors, were not accessible to unauthorized persons, and were protected by video surveillance systems and electronic door locks. The audit recommendations will help improve the physical security of the University’s information technology resources.

Isabel Benavides CIA, CGAP, CFE
Director, Audits and Consulting Services

Jose Gomez, MS
Information Systems Auditor III