Report on Encryption of University Information #13-201

We have completed our audit of Encryption of University Information. This audit was performed at the request of UT System and was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.

BACKGROUND

In 2007, The University of Texas System (Administration) issued a bulletin, “Encryption Practices for Storage of Confidential University Data on Portable and Non-University Owned Computing Devices (SPB-1),” which lays out the basic expectations and requirements for the encryption of laptop computers at UT System. However, in 2007 no single solution was available to encrypt all laptop platforms and many institutions did not readily adopt a solution. Since 2007, UT System has experienced several incidents of lost or stolen laptops containing confidential or sensitive data. As a result, the Executive Vice Chancellors in Health Affairs and Academic Affairs issued a memo to each institutional president, which required all institutions to report their current state of laptop encryption and their plan to encrypt all laptops. The memo required each institution to report this information by July 1, 2012.

In August 2012, many Information Technology (IT) departments struggled to accurately report all of their IT laptops. Several weakness related to the IT asset management processes at our institutions were identified. As a result, the UT System Audit Office asked each institution to include fiscal year 2013 audit plan hours to report on the status of laptop encryption and the adequacy of IT inventory controls at their institution.

OBJECTIVES

The objectives of this audit were to determine if all laptops used to conduct University business, whether University owned, leased, or employee owned have been appropriately encrypted, or exempted; to determine if the laptop inventory is complete, accurate and up to date; and to determine if the IT inventory processes are adequate to track and record inventory.

SCOPE AND METHODOLOGY

UT System provided Auditing and Advisory Services (A&AS) the program for this audit. As outlined in the program, A&AS reviewed the process for maintaining laptop inventory, IT inventory, and encrypting laptop computers at UTHealth. Through inquiry, sampling, and review of documentation, we reviewed key controls associated with the laptop inventory, IT inventory, and laptop encryption processes.
AUDIT RESULTS

Status Reported to UT System
UTH ealth reported to UT System that all but 6 of the known laptops were encrypted. UTH ealth submitted the appropriate exemptions to UT System in February 2013 and UT System accepted the exemption requests.

Encryption and Inventory Processes
A&AS reviewed the process for encrypting and monitoring the encryption of laptops and the process for maintaining laptop and IT inventory. During our work, we noted that the process for issuing and ultimately encrypting a laptop is decentralized and delegated to each IT department. As a result, the process for encryption, the encryption tools used and the inventory process varied. In order to understand the processes, A&AS audited nine different areas that included the following departments: Capital Asset Management (CAM), Information Security, Children’s Learning Institute, Harris County Psychiatric Center Management Information Systems, General Administration Information Technology, Graduate School of Biomedical Sciences Information Technology, Medical School Information Technology, School of Biomedical Informatics Information Technology Services, and the School of Public Health Information Technology Services. Due to the decentralized nature of UTH ealth’s IT organization, the integrity of both the encryption and inventory processes is dependent upon the local IT administrator.

UTH ealth started encrypting laptops in 2007. Due to the wide variety of operating system platforms supported by our IT organizations, changes in the suggested primary encryption solution, changes in technology, departments using different encryption solutions, and budget restrictions, multiple encryption products are currently in use. We reviewed six different encryption products that were in use as part of our encryption sample. Based upon review of IT policy and inquiry with the CISO, all encryption products used are acceptable.

Most areas are transitioning to a UT System endorsed encryption product, SecureDoc, that will provide increased monitoring capabilities for encrypted laptops. The conversion will occur over the next two to three years as the laptop population is refreshed (replaced).

One school’s IT department does not intend to use the encryption solution that the rest of the institution is adopting. This school prefers to use a Microsoft product, Bitlocker. This product does not have the same reporting capability as SecureDoc. Bitlocker cannot provide reports of machines that are no longer encrypted. The school cites that SecureDoc was developed by a small company and support for the product might be jeopardized if the company is acquired by a larger company.

Some areas of the institution utilize computer configuration software that requires specific software to be installed on a machine before it can be placed into service. This process is called creating and installing an image. One area created a requirement within the configuration tool that prevents the loading of the image to a machine if encryption is not part of the image. Other areas have a manual process that is dependent upon the administrator’s remembering to install the encryption software.
Encryption of Laptops

Information technology policy (ITPOL-007) Laptop Security Policy states “Non-university owned laptops should not be used under any circumstances to store University confidential data.” Based on this policy, the institution does not encrypt personally owned laptops.

A&AS selected a sample of 50 laptops for testing to identify whether the computers were encrypted, as evidenced through machine settings and, if yes, was an approved product used. The sample was judgmentally selected to ensure each of the nine different areas in the institution were covered, with the sample including both owned and leased laptops. An additional five computers were selected from a visual observation during our on-site visits to verify they were included in the inventory, and were encrypted. All of the machines tested were encrypted.

As part of our testing, we checked the encryption tool used to confirm that an acceptable method of encryption was in place. No instances of unapproved encryption methods were found.

We noted that, in order to meet business needs, one school granted administrative access to users who are located on remote campuses and for special needs users such as researchers. This level of access allows users to make changes to the image of their computer including removing the encryption tool from the drive. IT Pol-032 states “The system should be configured in a manner which prohibits the user from unencrypting the drive.” We were informed that many of the users signed an agreement stating they would not unencrypt their laptops.

Recommendation 1:

We recommend that Information Technology ensure that users do not have the ability to unencrypt a machine. We recommend that Information Technology initiate controls that ensure users do not have the ability to unencrypt a machine when it is necessary to provide users with administrative access. An information security exception request should be filed for all machines that cannot meet IT Pol-032’s requirement to prohibit a user’s ability to decrypt a machine.

Management's Response: The School of Public Health has the option of 1.) Filing an information security exception request for users/equipment that can be unencrypted by the end user; 2.) Providing for automatic notification when a machine is unencrypted by an end user; or 3.) Preventing the end user from being able to unencrypt the equipment. Derek Drewhorn, Assistant Dean for Information Technology, will direct this activity under the oversight of the CIO.

Responsible Party: Derek Drewhorn, Assistant Dean for Information Technology SPH
Implementation Date: April 1, 2014

We selected a sample of laptops from the total inventory to ensure that encryption keys were properly stored (escrowed). The escrowing of encryption keys allows data to be recovered and provides proof of encryption when a machine is lost or stolen. From our sample of 22, encryption keys were not escrowed for 4 laptops. In our discussions with IT management in one school, we were told that in place of escrowing keys for computers located in remote locations, a letter from the user stating the computer was encrypted was used. By not escrowing the

Encryption Key - An encryption key may encrypt (hide the meaning of information), decrypt, or perform both functions. Think of the encryption key as the password, code, or trigger needed to apply the mathematical operations used to encrypt and decrypt information.
encryption key, UTHealth does not have evidence the computer was encrypted, nor can the data stored on the computer be recovered. We obtained evidence that the four computers without escrowed encryption keys were encrypted.

During our test work, we noted areas that had escrowed keys, but had difficulty in locating where they were stored.

**Recommendation 2:**
We recommend that Information Technology conduct a review to ensure that every machine has an escrowed encryption key, and that the existence of an escrowed encryption key be tied to the computer inventory.

**Management’s Response:** SecureDoc automatically escrows the encryption key so equipment encrypted with other technology, including BitLocker and File Vault (for Apple equipment), will be reviewed against the equipment inventory for the area. The two major areas involved are the School of Public Health for BitLocker and the Medical School for File Vault. Derek Drawhorn and Bassel Choucair will provide confirmation under the oversight of the CIO. The other areas will provide confirmation to the CIO through their respective IT managers.

**Responsible Party:** Rick Miller, CIO  
**Implementation Date:** April 1, 2014

In addition, we noted that 340 machines were encrypted with the SafeBoot product. UTHealth has not renewed the SafeBoot licensing agreement. Without proper support, the needed recovery keys may not be available and data recovery is not guaranteed. According to UTHealth’s policy, ITPOL-032, and UT System policy, SPB 1, all encrypted machines must be encrypted with methods that ensure that encryption keys and recovery codes are maintained.

**Recommendation 3:**
We recommend that Information Technology take steps to address the risks associated with encrypting information with SafeBoot.

**Management’s Response:** SafeBoot is no longer used so as equipment is replaced, new equipment will be encrypted using another method, usually SecureDoc. In the interim, users will be informed that IT cannot recover unencrypted storage if a failure were to occur. IT staff will assist users in using other options to reduce the risk of data loss including: 1.) Storing data on shared storage systems (this is already a requirement in some areas), 2.) Backing up data to a secure device, or 3.) Utilizing an IT provided backup service. The CISO will monitor the status and review all exception requests for equipment still using SafeBoot after September 1, 2014.

**Responsible Party:** Rick Miller, CIO & Amar Yousif, CISO  
**Implementation Date:** September 1, 2014

**Desktop Encryption**
A similar requirement for the encryption of desktops will go into effect in March 2014. Based upon documentation provided by IT, UTHealth encrypted approximately 5000 desktops as of the time of our review.
Inventory
CAM maintains UTHealth’s official record of capital and controlled assets. This record does not include IT assets costing less than $500 or those assets which are leased. This policy omits at least 2500 university owned laptops from the CAM inventory that are currently in use. IT maintains a separate inventory to monitor the deployment of IT equipment.

Capital asset* - Is an asset that is valued at $5000.00 or more.
Controlled Asset* - For the purpose of this audit, is an asset that is classified as a computer, printer, or laptop and is valued at $500.00 or more.
*As defined by the State of Texas.

The process for maintaining the IT inventory is distributed across the individual IT departments and schools with little direction for standardization. The process involves little or no coordination with CAM to ensure completeness of either inventory. In one department, at least 35 individuals share responsibility for maintaining inventory. From the work we performed, we were able to identify laptops listed on the CAM inventory that were not on the IT inventory list and vice versa.

A&AS performed work to compare the CAM inventory against the IT inventory to reconcile capital and controlled assets between the two lists for completeness. Since the IT inventory process is decentralized, the inventory records vary to such a degree that compilation of the individual lists into one list for use in performing the reconciliation was not reasonably possible. Based on our inquiry, most departments do not consider the CAM list for inventory purposes when reporting on the status of encrypting laptop computers.

We also performed work to reconcile the inventories of leased laptops to the leasing company’s source documents. We were unable to reconcile the leasing company inventory against one department’s records. In our discussions, we were informed that not all areas reconcile their inventories of leased laptops to the leasing company’s source documents.

Because the inventory process is decentralized and lacks sufficient standardization to consolidate or reconcile many parts of the inventory against source documentation, we were unable to obtain reasonable assurance that the inventory lists are accurate.

Recommendation 4:
We recommend that CAM and Information Technology work together to develop a cooperative process that will ensure the official listing of capital and controlled assets is complete. As part of this cooperative effort, Information Technology management should develop a standardized IT inventory process to be followed by all of the institution’s information technology functions. The revisions to the IT inventory process should, at a minimum, include the following:

1. Centralize IT oversight and coordination for all IT assets, owned, and leased.
2. Create a common set of attributes (baseline attributes) that can be used to link all inventory tracking systems, including the CAM inventory.
3. Provide timely information to CAM that will allow reconciliation of university owned IT inventory.
4. Periodically reconcile all leased inventory as defined by centralized IT oversight.
5. Create the means to ensure timely transfer of obsolete equipment from the IT inventory.
6. Work with CAM to explore IT inventory process improvements and/or opportunities for automation.
7. Redefine a controlled IT asset to reflect the value of the information stored by the device and the risk to the institution.

Management's Response: Capital asset systems have traditionally served the financial functions (management of capital assets) of an institution rather than the information technology functions (location, configuration, usage, ownership, etc.). Information Technology has been evaluating a cloud based tool for managing IT services that includes a module for IT equipment inventory. IT will expand and continue the evaluation of services and software which will provide a campus-wide platform for keeping track of IT equipment. Capital Assets Management will participate in the process and lead the effort with respect to properly accounting for IT assets in the financial system as dictated by the state comptroller's office. This is a very large project that will include the evaluation, selection and implementation of software and services. The project will include conversion of records from many spreadsheets and systems within the schools, reconciliation of the data, a physical inventory as required, a transfer of primary responsibility for IT inventory to the Information Technology departments, and the development of new policies and procedures. Additional staffing and funding for software and/or services will be required.

Responsible Party: Rick Miller & Mike Tramonte
Implementation Date: September 1, 2014

CONCLUSION
All laptops sampled as part of this audit were encrypted as of the time of our review. A&AS noted areas for improvement for the IT inventory and encryption processes.

We would like to thank Capital Asset Management, Information Security, and the individual IT departments including: Harris County Psychiatric Center Management Information Systems, General Administration Information Technology, Graduate School of Biomedical Sciences Information Technology, Medical School Information Technology, School of Biomedical Informatics Information Technology Services, and the School of Public Health Information Technology Services for their assistance during our review.

Daniel G. Sherman, MBA, CPA CIA
Assistant Vice President

DGS:twb

cc: Audit Committee
Kevin Dillon
Mike Tramonte
Rick Miller
Amar Yousif

Audit Manager: Tim Burr, MBA, CIA, CISA, CFE
Auditor Assigned: Lieu Tran

Issue Date: August 9, 2013
Memorandum

To: Giuseppe N. Colasurdo, M.D.
    President

From: Daniel G. Sherman
      Assistant Vice President

Date: June 14, 2013

Re: Report on Audit Number 13-112 ARP/ATP

We have completed our audit of Advanced Research Programs/ Advanced Technology Program (ARP/ATP). This work was required by the Texas Higher Education Coordinating Board (THECB) and was part of our fiscal year 2013 audit plan. All work was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.

The scope of this audit is all ARP/ATP awards in the fiscal year 2012-2013 award cycle. The objective of this work is to provide organizational accountability of award funds. Our work revealed that there were no grants awarded to UTHealth in the fiscal year 2012-2013 award cycle.

DGS:cs

cc: Audit Committee