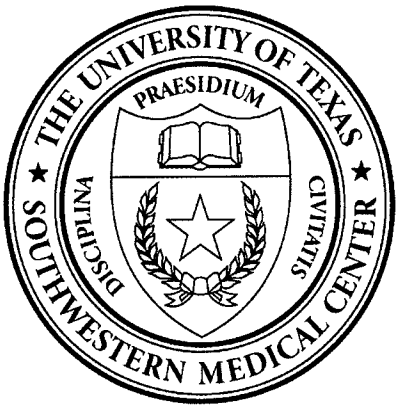
University of Texas Southwestern Medical Center

Internal Audit Report 13:21
Laptop Encryption Initiative Review



August 20, 2013

Office of Internal Audit
5323 Harry Hines Boulevard
Dallas, Texas 75390-9017
(214) 648-6106

University of Texas Southwestern Medical Center
Internal Audit Report 13:21
Laptop Encryption Initiative Review
FY 2013

AUDIT REPORT
August 20, 2013

Daniel K. Podolsky, M.D., President
University of Texas Southwestern Medical Center
5323 Harry Hines Boulevard, MC 9002
Dallas, Texas 75390-9002

Dear Dr. Podolsky:

The University of Texas Southwestern Medical Center (Medical Center) Office of Internal Audit has completed its review of the Medical Center Laptop Encryption Initiative.

Executive Summary

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 laid out the basic expectations and requirements for the encryption of laptop computers within the UT System. On June 20, 2012, the UT System Executive Vice Chancellor for Health Affairs issued a memorandum requiring each campus to encrypt 100% of Institution laptop computers as well as all personally owned laptops used to conduct any Institution business or containing sensitive information. This mandate set a target goal of 100% encryption rate of all Institution and personally owned laptops by August 31, 2012. The UT System Audit Office has requested each Institution to report on the encryption status in FY13.

The primary objectives of this review were to 1) determine whether Medical Center laptops have been properly encrypted or exempted from encryption per the Medical Center Laptop Encryption Initiative as mandated by the University of Texas System; and 2) determine whether laptop inventory at the Medical Center is complete, accurate, and up-to-date.

As a result of this audit, the following observations and recommendations are made to help the Medical Center achieve this compliance mandate.

Laptop Encryption Compliance Requirement

The Medical Center was not compliant with the mandated encryption rate of 100% of all laptops. In our review of 60 laptops selected for testing, three (5%) were not encrypted nor deemed exempt from encryption. This review was performed by sampling laptops on the campus and laptops appearing in the PeopleSoft Inventory Report produced by Material Management Group (Inventory Management Database). Since the sample was based on the *known* population of laptops owned by the Medical Center and not the broader number and higher risk laptops departmentally managed and personally owned, the actual error rate and risk impact may be greater than identified in the sample.

Upon discovery, management immediately remedied the three non-compliant computers. However, more work is required to ensure encryption for non-IR controlled (departmental) laptops. Specifically, IR should request each department identify what laptops exist with serial numbers and usage (active/inactive) defined so that appropriate encryption exists. Working with Inventory Control in this process is also recommended. Finally, this can be followed up as part of the decentralized IT project planned by Internal Audit in FY14.

Laptop Inventory Management Control

The Medical Center does not have a reliable mechanism in place to produce an inventory of all laptops subject to the encryption mandates. Because the current environment allows for departments outside of Information Resources (IR) to purchase and deploy laptops, appropriate governance does not exist to ensure ongoing compliance.
Further, we noted:

- PeopleSoft Inventory Report had quality/accuracy issues (missing serial numbers, obsolete and scrap included in population, personal laptops and laptops purchased outside of PeopleSoft not included in population), and
- Several departments were retaining obsolete laptop inventory rather than returning these machines to Inventory Control.

There is a potentially unknown/higher risk population of laptops not centrally managed by IR that could exist. We recommend that management perform the following:

- Develop stronger inventory controls and monitoring of laptop inventory to provide a full accounting of laptops subject to the encryption mandate. These controls should address governance, purchasing, use, retirement and destruction of relevant equipment.
- Inventory Control and IR Management should work with each department to reconcile PeopleSoft records to actual Medical Center inventory and KACE records to PeopleSoft and those laptops subject to encryption (Medical Center and personally owned).
- Enhance inventory input and quality control within PeopleSoft and review and improve quality procedures around the current periodic physical inventories to ensure reconciliation of maintained inventory with physical laptops deployed and in use.

Non-IR Laptops may exist without encryption monitoring program (KACE)

In non-IR managed areas, the electronic program (KACE) used to monitor encryption on laptops and computing devices accessing the critical Medical Center network were only required by policy and have not been monitored and enforced (as this exists with IR managed laptops). Recommendations include:

- Implement and enforce KACE on all high risk computing devices accessing the Medical Center network. Such enforcement should also ensure the inability of end users or departments to by-pass KACE.
- Continue focusing on educating departments and staff on relevant security policies, initiatives, and requirements.
- Enhance the monitoring and enforcement of current policies and discipline non-compliance where appropriate.

Management has reviewed, commented, and agreed on the recommendations made. We appreciate the professional courtesy and cooperation of the Information Resource and Inventory Control staff in assisting us with our audit and solutions.

Detailed Results

Individual results and recommendations are discussed below:

1. Laptop Encryption Compliance Requirement

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 laid out the basic expectations and requirements for the encryption of laptop computers within the UT System. Further to this bulletin, on June 20, 2012, the UT System Executive Vice Chancellor for Health Affairs issued a memorandum asking each campus to encrypt all Institution laptop computers as well as all personally owned computers used to conduct any Institution business or containing sensitive information. Many laptops within the system store sensitive information which must comply with regulatory requirements (i.e., FERPA, HIPAA, and PCI). The risk of sensitive information losing its confidentiality via stolen laptops is minimized through encryption which makes it imperative that all laptops go through the encryption process. This encryption mandate set a target goal of 100% encryption rate of Institution laptops by August 31, 2012.

The Medical Center was not compliant with the mandate of 100% encryption rate of Institution laptops. In our review, three out of the 60 laptops that were tested (5% of total population) were not encrypted nor were they exempt from encryption. The Medical Center has a decentralized IT environment with activity not centrally controlled by IR. As such, several departments are responsible for their own adherence to security policies (such as encryption) and the enforcement of these efforts may vary by department. Additionally, as the exact inventory of Institution laptops and personally owned laptops is not known, Management cannot demonstrate how they can currently meet the mandate given the existing control environment. Note, the population of Institution and personally owned laptops known to IR is estimated to be over 4500, and there may be a significant additional number of laptops which are not known to IR that may or may not meet the requirement of the mandate.

Upon discovery, management immediately remedied the three non-compliant computers. Even though these have been remedied, due to the sheer number of laptops subject to the mandate and the sample population's error rate, the likely number of actual machines that are not compliant may be significant.

The three laptops that were not encrypted are as follows:

1. Sample # 1: PS# 460418 (IR Health Systems)
   The laptop was taken out of service due to a failure during the encryption process. The device was not encrypted, but was in the process of being returned to Material Management.

2. Sample #19: PS# 448059 (MSRDP Billing Operations)
   The laptop was taken out of service due to a failure during the encryption process. Device was returned to Material Management due to malware and was never encrypted (encrypted failed due to malware).

3. Sample #43: PS# 461567 (Cardiology)
   This laptop developed issues in conjunction with the installation of KACE. Laptop was still in service and not encrypted or running KACE.

<u>Recommendation</u>

1. IR should put monitoring mechanisms in place to prevent laptops without KACE and appropriate encryption software from accessing the Medical Center network or storing, downloading, and transmitting any Medical Center sensitive information.

2. Management should develop controls and procedures that will automatically prompt the installation of KACE on all laptops attempting to access Medical Center's network or sensitive

data. If the installation is delayed, cancelled, or deleted, the laptop should not be allowed access to the network.

3. Management should continue their focus around educating departments and staff on relevant security policies, initiatives and requirements. Management should consider enhancing the enforcement of current policies and discipline noncompliance where appropriate.

4. Management should perform more work to ensure encryption for non-IR controlled (departmental) laptops. Specifically, IR should request each department identify what laptops exist with serial numbers and usage (active/inactive) defined so that appropriate encryption can exist.

Management Response

To greatly reduce failures during the encryption process, self-encrypting hard drives will be included as the standard in all supported IR workstation purchases and will be strongly recommended for all UT Southwestern purchases.

Target Implementation Date: September 30, 2013

The Health System is actively testing controls that would prevent non-compliant computers from connecting to the Health System network or accessing key Health System information. The initial project has been funded as a FY14 project.

Target Implementation Date: FY14

In addition to laptop encryption, IR is implementing additional security controls that further reduce risks from personally owned mobile devices and portable storage devices.

Responsible Party:
Joshua Spencer, Chief Information Security Officer

2. Laptop Inventory Management Control

The Medical Center does not have a reliable mechanism in place to produce an inventory of all laptops subject to the encryption mandates. Because the current environment allows for departments outside of Information Resources (IR) to purchase and deploy laptops, appropriate governance does not exist to ensure ongoing compliance. Further, we noted:

- PeopleSoft Inventory Report had quality/accuracy issues (missing serial numbers, obsolete/scrap included in population, personal laptops and laptops purchased outside of PeopleSoft not included in population); and
- Several departments were retaining obsolete laptop inventory rather than returning these machines to Inventory Control.

Recommendations:

We recommend that management perform the following:

- Develop stronger inventory controls and monitoring of laptop inventory to provide a full accounting of laptops subject to the encryption mandate. These controls should address governance, purchasing, use, retirement and destruction of relevant equipment.
- Inventory Control and IR Management should work with each department to reconcile PeopleSoft records to actual Medical Center inventory and KACE records to PeopleSoft and those laptops subject to encryption (Medical Center and personally owned).

- Enhance inventory input and quality controls within PeopleSoft and review and improve quality procedures around the current periodic physical inventories to ensure reconciliation of maintained inventory with physical laptops deployed and in use.

Management Response

Medical Center laptops are not currently required to be purchased through a central and controlled purchasing process. Additionally, non-IR personnel are allowed administrative access rights to their devices, allowing them to remove any installed software. These factors prevent assurance that all laptops will be encrypted. A strategic initiative is underway to determine the role of IR in departmental computing. The impact and resources required to guarantee security configuration of all devices will be presented to Executive Leadership to approve implementation of these controls or acceptance of the risks.

Additionally, Gary Quinn, Manager of Inventory Control, (with the support of Paul Belew, AVP-Materials Management) agreed to work with IR to resolve inventory accuracy matters as discussed.

Target Implementation Date: December 31, 2013

Responsible Party:
Joshua Spencer, Chief Information Security Officer
Gary Quinn, Manager of Inventory Control, Materials Management (suppoted by Paul Belew, AVP, Materials Management)

3. Non-IR Laptops may exist without encryption monitoring program (KACE)

IR has been utilizing DELL KACE (KACE) to help identify the population of laptops that are accessing the Medical Center network and require encryption. KACE is an IT inventory management and device discovery application which monitors the device's configuration for computers that it is installed—which includes the encryption state of the computer. KACE currently is not a prerequisite to access the Medical Center network and it can be deleted, modified, or bypassed by laptops that are not centrally monitored by IR (i.e., personal laptops, research laptops and other departmental laptops). This prevents IR from having oversight into the security configuration of these devices and also prevents IR from being able to validate encryption status. These limitations have resulted in an inaccurate and incomplete population of laptops that require encryption per the mandate and individuals may access sensitive Medical Center data on personal laptops and non-encrypted laptops. Finally, because the Medical Center IT environment is decentralized and non-IR individuals are granted administrative access on department devices and personal devices, end users and departments have the ability to remove installed software or prevent downloads of required system applications (i.e., KACE).

Recommendation

Recommendations include:

- Require all Medical Center laptops and computing devices connecting to the Medical Center network to require the use of KACE (or an equivalent tool). Medical Center computing devices not containing such software should not be allowed any level of access to the network. When a device attempts to connect to the network without KACE installed, we recommend that users are prompted by a notification which informs them of policies and provides the user a link to install KACE for all laptop devices.
- Enhance the role of IR in departmental computing including restricting administrative access rights on laptops to IR employees only and removing administrative access rights to laptops for non-IR employees.
- Continue focusing on educating departments and staff on relevant security policies, initiatives, and requirements.
  Enhance the monitoring and enforcement of current policies and discipline non-compliance where appropriate.

Management Response

Medical Center laptops are not currently required to be purchased through a central and controlled purchasing process. Additionally, non-IR personnel are allowed administrative access rights to their devices, allowing them to remove any installed software. These factors prevent assurance that all laptops will be encrypted. A strategic initiative is underway to determine the role of IR in departmental computing. The impact and resources required to guarantee security configuration of all devices will be presented to Executive Leadership to approve implementation of these controls or acceptance of the risks.

Target Implementation Date: September 30, 2013

Responsible Party:
Joshua Spencer, Chief Information Security Officer

Sincerely,

Chris Dugas, PwC Internal Audit Services

Daniel Fontenot, PwC Internal Audit Services

Debbie McKibben, PwC Internal Audit Services

Cc: Arnim E. Dontes, MBA, Executive Vice President for Business Affairs
Joshua Spencer, CPHIMS, CISSP, Chief Information Security Officer
Paul Belew, AVP, Materials Management

Appendix

Background

A review of the Medical Center Laptop Encryption Initiative was included in the FY 2013 internal audit plan, which is based on the Internal Audit risk assessment process and approved by the Audit Committee of the Board of Trustees.

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. On June 20, 2012, the Executive Vice Chancellor for Health Affairs issued a memorandum 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.

For FY 2013, the System Audit office asked each Institution to include audit plan hours to report on the status of encryption at their Institution.

Audit Objectives

The primary objectives of this review were to 1) determine whether laptop inventory at the Medical Center is complete, accurate, and up-to-date; and 2) determine whether all Institutional laptops have been properly encrypted or exempted from encryption per the Medical Center Laptop Encryption Initiative.

To accomplish this internal audit, we obtained an understanding of Laptop Encryption Initiative process. This was done primarily through interviews with personnel and review of documents and/or limited testing of laptops.

Scope and Methodology

Our audit covered the Laptop Encryption Initiative which covered all Institutional laptop computers (including personal computers that faculty or staff may use to conduct any Institution business). This is a Medical Center required audit from the fiscal year 2013 Medical Center Audit Plan. Our examination was conducted according to guidelines set forth by the University of Texas Systems Policy 129 "Internal Audit Activities", the Regents Rules and Regulations and the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing*. The scope of this review did not include encryption efforts around other mobile computing devices such as iPhone, iPad, or USB devices or the ability to move sensitive data to other devices through the use of USB devices, disk or transmission via email.

Procedures conducted to satisfy the audit objectives included the following:

- Examined the Executive Vice Chancellor's Encryption Memo
- Examined the system-wide encryption bulletin which is located at the following website: http://utsystem.edu/ciso/spb1.pdf
- Reviewed the laptop encryption initiative website
- Interviewed employees of the various areas related to the Laptop Encryption Initiative (Information Systems, IR and Material Management) and documented the actual procedures undertaken and operational processes.
- Obtained the laptop inventory population from Material Management (PS Inventory Report) and list of encrypted laptops from Information Systems (DELL KACE Crystal Report).

- Performed reconciliation between the People Soft inventory Report and the Dell KACE Crystal Report. Variances Existed.

- Analyzed laptop inventory and considered high risk departments and high risk employees such as faculty laptops where student data is likely to exist. Additionally, interviewed IR personnel to determine higher risk departments and areas of focus. Based on analysis and interviews, a sample of 14 departments were selected for further review based on the following factors:

    - Number of records within a department,
    - FERPA
    - HIPAA,
    - PCI-DSS (credit card information), and
    - Other confidential information and regulations.

- A total of 60 laptops were haphazardly selected for testing. This sample was selected from 14 higher risk departments which were identified through discussions with IR personnel.

    - Randomly selected 35 laptops (across 14 higher risk departments) and inspected the selected laptops for evidence of full disk encryption and verified compliance with the Laptop Encryption Initiative.

    - Randomly selected 20 additional laptops that were located in the selected 14 departments and verified that they were on the PS Inventory Report and Dell KACE Crystal Report. Additionally, inspected these laptops for evidence of full disk encryption and verified compliance with the Laptop Encryption Initiative.

    - Sampled five laptops from a list of exempted laptops and verified that these exempted laptops were appropriately excluded from encryption and that they were appropriately approved for exempt status.

    - Obtained supporting documentation and evidence for non-encrypted laptops that were not approved for exemption. Verified the unencrypted laptops did not contain confidential data or other safeguards were taken to the reduce risk of lost or stolen sensitive Medical Center information. Additionally, interviewed laptop owners to verify what, if any, confidential information was stored on the laptop.

Our work was substantially completed by April 3, 2013 with follow up recommendations identified and finalized by August 20, 2013.