The University of Texas System
Nine Universities. Six Health Institutions. Unlimited Possibilities.

System Audit Office
210 W. 6th Street, Suite B.140E, Austin, Texas 78701
Phone: 512-499-4390 Fax: 512-499-4426

July 6, 2015

Phillip B. Dendy
Executive Director of Risk Management and Systemwide Compliance Officer *ad interim*
The University of Texas System Administration
210 W. 6th Street, Suite B.140E
Austin, Texas 78701

Dear Mr. Dendy:

We have completed our audit of mobile device management across The University of Texas System. The detailed report is attached for your review.

We conducted our engagement in accordance with The Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing*.

We will follow up on recommendations made in this report to determine their implementation status. This process will help enhance accountability and ensure that audit recommendations are implemented in a timely manner.

We appreciate the assistance provided by all information security staff and other personnel throughout this audit.

Sincerely,

J. Michael Peppers, CPA, CIA, QIAL, CRMA
Chief Audit Executive

cc: Mr. Miguel Soldi, Assistant CISO - Policy and Administration
Mr. Kevin Kjosa, Assistant CISO - Technical Support
Mr. Marc Milstein, Associate Vice Chancellor and Chief Information Officer
Institutional Chief Audit Executives
Institutional Chief Information Security Officers

The University of Texas System
Mobile Device Management Audit Report
FY 2015

July 2015

THE UNIVERSITY OF TEXAS SYSTEM AUDIT OFFICE
210 WEST SIXTH STREET, SUITE B.140E
AUSTIN, TX 78701
(512) 499-4390

Audit Report

July 2015

EXECUTIVE SUMMARY

In a November 2011 report to The University of Texas (UT) System Board of Regents (Board), Deloitte & Touche LLP (Deloitte) cited mobile device security as the top security risk Systemwide. Mobile devices, particularly those owned by individuals instead of the institution, present a high risk to information security due to the widespread and increased use of mobile devices to access University information resources by UT System faculty, staff, and students, who may not be aware of best practices or have the tools to securely use such devices. In addition to the risk that University confidential data may reside on a personally-owned and unsecure mobile device, connecting an unmonitored or unmanaged device to institutional resources also increases the risk of spreading malware and other network intrusion threats. These risks may be somewhat mitigated by having some combination of user training and security and monitoring operations at each institution. The impact of a failure to manage institutionally-owned and personally-owned mobile devices (collectively referred to as mobile devices unless specifically stated otherwise) could vary, depending on the specific situation and whether any confidential or sensitive data was compromised.

The Deloitte security report resulted in the development of the UT System Information Security Assurance Initiative (ISAI), and as of November 2014, slightly over $1 million allocated for this initiative had been spent specifically towards mobile device security. The majority of the mobile device security funds were used to purchase Systemwide licenses for a mobile device management (MDM) software solution, AirWatch LLC.

To determine whether UT System institutions are implementing appropriate strategies to address these risks, we read policies and procedures related to mobile devices and interviewed institutional Chief Information Security Officers (CISOs). We also reviewed UT System's agreement with AirWatch, LLC to gain an understanding of the contract terms for the purchase of MDM services, and assessed implementation status of this solution.

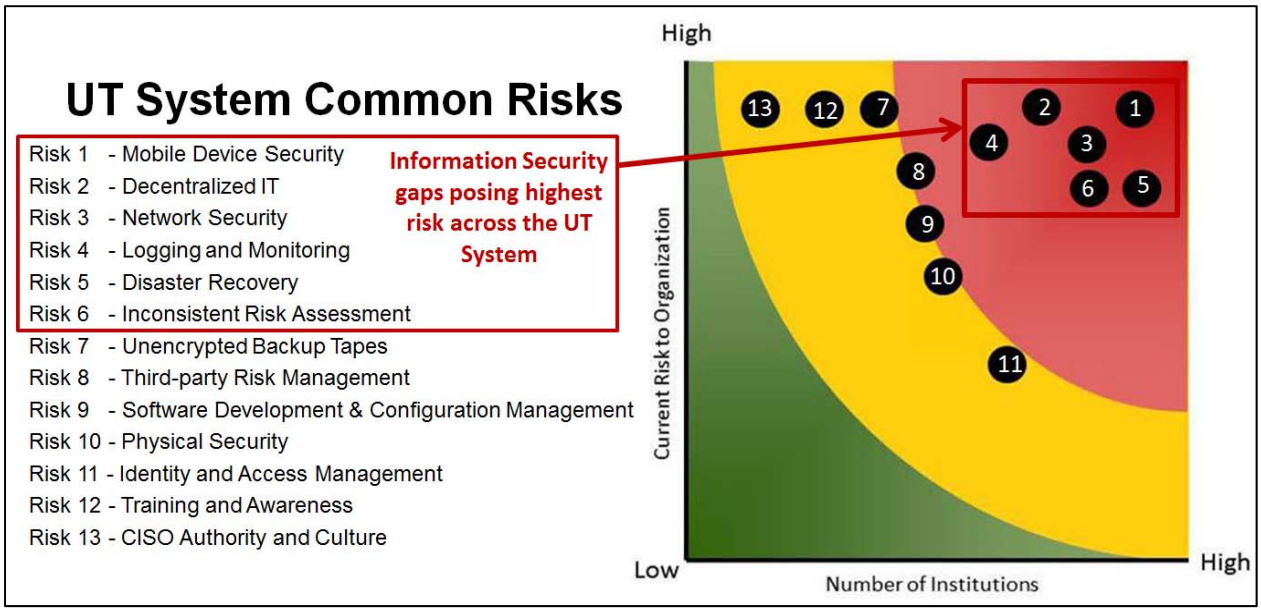
Information security staff are aware of the rise in mobile device usage across the UT System. Institutions are currently in various stages of maturity in terms of mobile device management strategy, ranging from limited controls up through more robust MDM solutions. This report includes recommendations related to enhancing coverage of mobile device topics in policies and procedures, inventorying mobile devices, managing the AirWatch contract, and additional observations regarding cloud storage and computing services that are common with mobile device use.

A Priority Finding is defined as "*an issue identified by an internal audit that, if not addressed timely, could directly impact achievement of a strategic or important operational objective of a UT institution or the UT System as a whole.*" Non-Priority Findings are ranked as High, Medium, or Low, with the level of significance based on an assessment of applicable Qualitative, Operational Control, and Quantitative risk factors and probability of a negative outcome occurring if the risk is not adequately mitigated. This audit resulted in one High and three Medium-level findings, but no Priority Findings.

BACKGROUND

In November 2011, following a report to the Board by Deloitte on their comprehensive information security compliance effectiveness review of UT System, the Board allocated $29,255,000 to invest in various information security enhancements. This launched the UT System Information Security

Assurance Initiative, and as of November 2014, slightly over $1 million had been used towards mobile device security, specifically by purchasing the AirWatch MDM software. The rest of the ISAI allocation was budgeted for other information security risks identified by Deloitte. As shown in the following graphic, mobile device security was identified by Deloitte as the highest security risk across UT System. Accordingly, the UT Systemwide Information Security Office recognized this risk and attempted to mitigate it with an MDM solution that could be used across the institutions.



Graphic courtesy of the UT Systemwide Information Security Office

Since mobile device security was identified as the highest security risk, institutional policies should clarify what constitutes a mobile device or refer institutional users to UT System Policy UTS165, *Information Resources Use and Security Policy*. The National Institute of Standards and Technology (NIST) acknowledges the difficulty in defining a "mobile device" because their features are constantly changing. However, in its Special Publication 800-124, Revision 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, NIST does provide a working definition of a mobile device as one that has:

- A small form factor;
- At least one wireless network interface for network access (data communications);
- Local built-in (non-removable) data storage;
- An operating system that is not a full-fledged desktop or laptop operating system; and
- Applications available through multiple methods (provided with the mobile device, accessed through web browser, acquired and installed from third parties).

Additionally, the provisions of the *Texas Administrative Code*, Title 1, Part 10, Chapter 202 (TAC 202) that became effective on March 17, 2015 require the Texas Department of Information Resources (DIR) to define mandatory security controls. Recognizing that "mobile computing and teleworking expose systems and information to exploitable vulnerabilities," the DIR published the *Security Control Standards Catalog* and established control standard AC-19 – Access Control for Mobile Devices, which requires that state organizations begin implementing "usage restrictions, configuration requirements, connection

requirements, and implementation guidance for organization-controlled mobile devices, whether owned by the state organization or the employee" by February 2016. These requirements should be taken into consideration when updating or developing new institutional policies regarding mobile devices.

Contributing to the risk is the fact that use of mobile devices has increased rapidly over the past several years, beyond personal use for gaming or entertainment, to a broad spectrum of both personal and corporate computing and connectivity. Gartner, an information technology (IT) research and advisory company, issued a press release on January 5, 2015[1], predicting an increase in the number of overall computing device shipments through 2016; however, traditional personal computers (PCs) are expected to decrease, while "ultramobile" PCs, tablets, mobile phones, and other hybrid computing devices are expected to increase. Summary data on the current mobile landscape is presented in the following table:

Worldwide Device Shipments by Segment, 2014-2016 (Millions of Units)			
Device Type	**2014 Estimated**	**2015 Projected**	**2016 Projected**
Traditional Personal Computers (PCs), Desk-Based and Notebook	279	259	248
Ultramobile Premium	39	62	85
PC Market Total	**318**	**321**	**333**
Tablets	216	233	259
Mobile Phones	1,838	1,906	1,969
Other Hybrids/Clamshells	6	9	11
Total	**2,378**	**2,469**	**2,572**

As indicated from these data, the use of mobile devices is expected to rise. While protecting data is critical, the increase of mobile devices being connected to institutional networks also introduces a new source for attacks. Therefore, the proliferation of mobile devices and their increased use to access University information resources was identified as a high risk and, combined with the Deloitte security findings, resulted in the inclusion of this audit on the Fiscal Year 2015 audit plan.

AUDIT OBJECTIVES

The objectives of this audit were to assess whether UT institutions, including UT System Administration, have a) policies and procedures in place to define and address mobile devices and b) methods to enforce these policies and manage such devices. We also gathered information on institutional successes and challenges in implementing mobile device management strategies.

SCOPE & METHODOLOGY

For purposes of this audit, we substantially adopted NIST's definition and focused on small devices that do not run on a full-fledged desktop or laptop operating system (i.e., primarily Android and Apple iOS smartphones and tablets). Also, institutionally-owned mobile devices are defined as devices purchased and managed by the institution, and personally-owned mobile devices are defined as those that are owned by individuals instead of the institution but used for business purposes. Policies and procedures related to institutionally-owned laptop computers were not included in the scope of this audit. Our review of UT System and institutional policies and procedures for coverage of mobile device security topics was based on guidance from various sources (for example, NIST and ISACA).

[1] "Gartner Says Tablet Sales Continue to Be Slow in 2015," Gartner, Inc., accessed March 2, 2015, http://www.gartner.com/newsroom/id/2954317.

We performed background research to gain an understanding of the current mobile device landscape and MDM technologies, and reviewed institutional policies and procedures for mobile devices. We gathered and reviewed information about mobile device security practices from the institutional CISOs through questionnaires and follow-up meetings. We also reviewed UT System's agreement with AirWatch to gain an understanding of the terms for the purchase of MDM services.

This audit was primarily intended to assess whether institutions across the UT System have a mobile device strategy in place, and if so, to what extent. Having a strategy, or plan, in place is an important first step to achieving effective mobile device security. Accordingly, we collected and analyzed information that was self-reported by the information security staff across UT System and did not perform specific detailed testing for compliance with institutional policies. That is, we inquired whether MDM was being used but did not test whether the MDM solution was in place and effectively functioning. Our audit was conducted in accordance with guidelines set forth in the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing.*

AUDIT RESULTS

The CISOs and their staff reported that a variety of mobile devices, such as phones and tablets, are used to check email and run various mobile device programs ("apps") for business purposes at their respective institutions. In general, the UT System institutions are currently in various stages of maturity in terms of mobile device management. As expected, some institutions had more mature mobile device management strategies than others. The AirWatch MDM solution that was purchased by UT System has not yet been fully leveraged by UT System Administration or the institutions, as described in further detail below. Generally, the health institutions had more robust strategies in place, while the smaller academic institutions tended to lag behind in implementation of MDM strategies, reportedly due to limited resources and different institutional needs.

Mobile Device Management Solutions

As previously mentioned, users increasingly rely on the use of mobile devices to stay connected to their business-related emails, calendar, and contacts. Most institutions allow personally-owned devices, with few restrictions, to connect to the institutional network, provided that the user has the appropriate credentials. For example, UT MD Anderson does not allow Android devices and will request that they be disconnected when detected and UTHSC-Houston does not permit jailbroken or rooted devices.[2] MDM software solutions can help enforce these restrictions.

MDM Products and Common Features

Implementation and use of MDM software varies among the institutions. The CISOs reported that they are evaluating or are currently using different tools for MDM, including:

- Absolute Manage
- AirWatch by VMware
- BoxTone (now Good Technology)
- Microsoft Intune
- Cisco Meraki
- MobileIron

[2] "Jailbreaking" or "rooting" a device is the process of removing or circumventing restrictions such that the user can modify the core operating system.

- AT&T Toggle
- Microsoft Exchange ActiveSync protocol

Note that Microsoft Exchange ActiveSync is a communications protocol for the synchronization of email and other information (for example, a user's emails, calendar, and contacts) from a server to users' mobile devices. While it is not generally considered a full MDM product, it does have some MDM capabilities and can be used to enforce certain security policies, such as requiring passwords and performing remote wipes.

An MDM product typically has more robust features and can perform more device management functions. For example, while ActiveSync can wipe a device remotely, MDM software may offer the option to only delete business-related data or only provide view access to emails such that they are never actually stored on the mobile device. MDM solutions in the market today offer security controls that can be applied to the entire device or only to a secure container on the device. According to Gartner, MDM "includes software that provides the following functions: software distribution, policy management, inventory management, security management and service management for smartphones and media tablets."[3]

We reviewed product information from various MDM vendors and found their software have certain features in common:

- Manage various types of devices running different operating systems;
- Provide visibility into enrolled devices from a single console or dashboard;
- Enforce network security policies and manage apps;
- Segregate work content from personal content; and
- Allow easy enrollment of personally-owned devices.

Unused AirWatch Licenses Purchased by UT System

In July 2013, UT System entered into a Preferred Supplier Agreement with AirWatch, LLC for MDM services. As part of this agreement, UT System purchased 50,000 perpetual licenses for the MDM software at $14 each and also received 10,000 perpetual licenses[4] for AirWatch's mobile content management (MCM) software without charge. The MCM software allows corporate content to be securely stored and accessed from mobile devices. UT System also paid for the first two years of annual maintenance and support for the MDM and one year of maintenance and support for the MCM (maintenance fees for the first year were waived), with the current maintenance term scheduled to expire at the end of July 2015. The annual maintenance fee for the MDM and MCM is $2.80 per license. The aggregate initial cost of the software licenses and maintenance was $1,008,000.

Item	Units	Price per Unit	Total
MDM License	50,000	$14.00	$700,000
MDM Annual Maintenance	50,000	$2.80/year	$280,000
MCM License	10,000	$0 (waived)	$0
MCM Annual Maintenance	10,000	$2.80/year	$28,000
Total			**$1,008,000**

[3] Gartner, Inc., accessed March 2, 2015, http://www.gartner.com/it-glossary/mobile-device-management-mdm.
[4] A perpetual license allows the licensed software to be used indefinitely. However, separate annual maintenance fees are typically required to receive updates to the software.

Beginning with the third year, any institutions that hold licenses will be responsible for maintenance fees on those licenses allocated to them. For any licenses not allocated, UT System is contractually obligated to pay for maintenance fees or the software will not be updated and become outdated as mobile devices and operating systems evolve.

The AirWatch contract was executed with the intent that the MDM tool would be made available for those institutions that did not already have an MDM tool in place. The implementation of AirWatch MDM was not mandated. Of the 50,000 AirWatch MDM licenses purchased by UT System nearly two years ago, approximately 22,500 (or 45 percent) have been requested by the institutions for deployment as of March 2015, leaving over half of the licenses remaining with UT System. Of the 22,566 licenses reported as requested[6], approximately 17 percent (or 8 percent of the 50,000 total) was reported as actually being in use. The table to the right provides a summary of the AirWatch MDM licenses requested, and being used, by each institution. This effectively translates to about $645,000 of MDM software and $258,000 in annual maintenance fees, or approximately $903,000 of the initial cost left unused Systemwide.

Institution	Requested	Used
UT Arlington	2,051	0
UT Austin	0	100[5]
UT San Antonio	100	0
UT Tyler	500	few
UT MD Anderson	100	0
UT Southwestern	1,815	1,442
UTHSC-Houston	7,000	2,009
UTHSC-San Antonio	5,000	62
UT Medical Branch	5,500	368
UT System Administration	500	6
Total	**22,566**	**3,887**

Recommendation (1): If a significant number of the licenses will remain unused, the Systemwide Information Security Office should work with the vendor to suspend the annual maintenance fees for unused licenses (currently approximately $75,000 per year) or identify a feasible alternative to mitigate the future expense (such as eliminating those licenses not expected to be used).

Level (1): This finding is considered **High** due to the actual costs incurred and potential future costs for a product that is not being significantly utilized.

Management's Response (1): As part of the ISAI initiative, the Systemwide Information Security Office created a multi-institutional work group, comprised of members from UT Dallas, UT Austin, UT Pan American, UT Southwestern, UT HSC Houston, Medical Branch, MDACC, and the Supply Chain Alliance, to determine the functional requirements of the product, determine deployment levels, draft a Request for Proposal (RFP), evaluate proposals, and make a recommendation on the selected product. The intent of the purchase of AirWatch was to provide those institutions that had not already selected and purchased a product with a viable alternative.

Institutions have the flexibility to choose a mobile device management product that best meets the institutions' requirements and capabilities of implementation. Institutions are not required by directive or policy to use or consider AirWatch as their preferred solution for mobile device management.

[5] Note that UT Austin's 100 AirWatch MDM licenses are excluded from the total, as those appear to have been purchased separately from the UT System agreement (on annual subscription basis), based on accounting records.
[6] The total number of licenses reported as requested by the institutions was substantially reconciled to an internal tracking spreadsheet provided by the Systemwide Information Security Office in March 2015 (within 282 licenses).

Management agrees with the need to avoid the continued payment of maintenance on licenses that will never be deployed. The Systemwide Information Security Office will work with VMware to identify a means by which UT System and institutions will pay for the maintenance of licenses deployed or that have a realistic expectation of being deployed in the short to medium term. Specifically:

- Determine the number of AirWatch licenses currently not allocated or deployed.
- Follow up with institutions to assess the status of their corresponding evaluations and deployment.
- Re-evaluate the number of licenses that will be required by institutions deploying or considering deploying AirWatch.
- Determine the number of excess licenses that, realistically, will never be deployed.
- Engage VMware in conversations to identify, if possible, a path moving forward by which the maintenance fee for the excess licenses is suspended or avoided.

Implementation Date (1): August 31st, 2015

Recommendation (2a, 2b): The Systemwide Information Security Office should continue to work with the CISOs of the institutions where AirWatch MDM is not being considered to reassess the viability of implementing that product. Also, it may be beneficial to develop awareness training to assist the institutional CISOs in better informing the users at their institutions of the capabilities and limitations of MDM, and how the features of an MDM solution will assist and protect the users. Recognizing that institutions may implement AirWatch in different ways, training content could include a general reminder of the importance of protecting University data and the purpose of MDM as another tool to do so. Communicating this message may increase success in deployment.

Level (2a, 2b): This finding is considered **Medium** due to potential level of information security risk from insufficient controls over mobile devices as their use is expected to increase over time.

Management's Response (2a): The recommendation includes a task related to the implementation of AirWatch and a task related to mobile device management awareness training. Each will be addressed separately.

The Systemwide Information Security Office has actively engaged institutions on mobile device management, including AirWatch. As mentioned above, institutions are not required by directive or policy to use AirWatch as their preferred solution for mobile device management. This recommendation requires the Systemwide Information Security Office to compel institutions not currently considering AirWatch to reassess their decision. However, the Systemwide Information Security Office will re-engage institutions that do not have an MDM strategy in place as identified in Appendix B.

Implementation Date (2a):

- Email communication to appropriate CISOs and follow-up conference call: July 31st.
- Include mobile device management implementation as topic of discussion during CISO Council – August 12th.
- In-person meeting and discussion during CISO Council and UTINFOSEC – August 14th.
- Report detailing outcome of communication and meeting – August 31st, 2015.

Management's Response (2b): Management agrees that training and guidelines are an important requirement for a successful implementation of a mobile device management strategy and to create the user buy-in needed to accept it, enroll devices, and participate in its deployment. The Systemwide Information Security Office leverages mobile device management related resources from UT System institutions, EDUCAUSE, and institutions of higher education, and makes them available to institutional CISOs via a SharePoint site dedicated to mobile device management. The items below are already works-in-process:

- Create a UT System web site for mobile device management that introduces the initiative and includes links to resources available to CISOs.
- Create a SharePoint site, as part of the UT System CISO SharePoint, dedicated to mobile device management that includes: benefits, FAQ, Getting Started guidelines, privacy concerns, configuration baselines, and resources from other UT System institutions, EDUCAUSE, and other institutions of higher education.
- Create a SharePoint site to support the UT System Administration AirWatch pilot implementation. In addition, this site will include device requirements, device enrollment instructions, and device management rules.

Implementation Date (2b): August 31st, 2015

AirWatch and MDM Usage Systemwide

Based on AirWatch's website materials and a review of the agreement, it appears that their MDM solution can control the majority of mobile device platforms (operating systems) currently in use and manage personally-owned mobile devices as well. The AirWatch MDM solution is in various stages of implementation across the UT System institutions, with UT Southwestern appearing to be the most fully implemented based on the information we reviewed. Several other institutions are evaluating or deploying the software, and a few have not been able to begin work on AirWatch or any other MDM implementation for various reasons. See ***Appendix B*** for details by institution, including explanations provided for why AirWatch was not implemented. A summary follows:

- 1 of 16 institutions[7] has fully implemented AirWatch;
- 7 institutions are evaluating or have partially implemented AirWatch and are planning to expand implementation;
- 3 institutions have fully implemented and were already using a different MDM solution (Absolute Manage, Meraki, and BoxTone);
- 4 institutions are evaluating or have partially implemented a different MDM solution; and
- 3 institutions do not yet have plans to implement any MDM solution.

At institutions where the purchased AirWatch licenses are not currently being considered for use, the institutional CISOs cited ongoing maintenance fees, inadequate staffing and training, and a desire for products that are more suited for their unique institutional needs as some of the reasons for not implementing AirWatch at this time. Interestingly, at two institutions where AirWatch is not being considered for implementation across the entire institution, each one has a single department that does use AirWatch for MDM.

[7] For purposes of this audit, UT System Administration was considered an institution, along with the nine current academic institutions and the six current health institutions. However, total number of institutions does not equal 16 because some institutions are evaluating AirWatch along with a different MDM solution.

UTS165 includes specific requirements for mobile devices used for business. Also, institutions may allow users to access or store confidential data with a personally-owned mobile device. The UT System Information Security Compliance staff conducted a series of "Mobility Monday" presentations to educate technical staff across the UT System about various risks related to mobile devices and using MDM software solutions. An MDM solution would help meet the policy requirements and mitigate risks related to unauthorized exposure of confidential data.

Recommendation (3): The Systemwide Information Security Office should assist the institutions in reconsidering a decision to not implement any MDM solution by highlighting how MDM can be used to enhance policy compliance and overall information security. While additional cost and effort may be required upfront, an MDM solution can help ensure compliance with policy requirements and mitigate risks related to unauthorized exposure of confidential data.

Level (3): This finding is considered **Medium** due to the potential level of information security risk from insufficient controls over mobile devices as their use is expected to increase over time.

Management's Response (3): Management agrees that the implementation of a mobile device management strategy and supporting application mitigates risks related to unauthorized exposure of confidential data, enhances policy compliance, and overall information security. The implementation of such a strategy and application is not a trivial endeavor limited to installing and deploying a tool, but one that requires policy work, identification of requirements and creation of management rules, strategy communication and socializing, creation of a device enrollment portal, installation and configuration of the application, help desk support, monitoring of the application and enforcement of rules, rules review and maintenance, etc., all of which require ongoing time and effort from information security and/or information technology staff. AirWatch could be available to those institutions at no cost to them and still they would not be able to successfully implement because they lack the staff and/or the budget to support the initiative.

The Systemwide Information Security Office will contact institutions identified in Appendix B to assess barriers to implementation of an mobile device management solution and determine the feasibility of implementing a targeted mobile device management strategy (e.g., high-priority departments or roles), leveraging AirWatch Software as a Service (SaaS) option and/or the use of Systemwide Information Security Office staff and resources to facilitate implementation.

Implementation Date (3): December 31st, 2015

Other MDM Considerations

In most cases, the CISO staff are responsible for providing policy guidance, and the IT staff are operationally responsible for implementing MDM software. One CISO cited this as a positive aspect of the implementation process. He believed that, because the information security group provided policy guidance and asked IT, which worked with mobile devices and the Exchange system, to be in charge of MDM implementation, it resulted in a better focus on product functionality for the end users. However, CISOs should continue to take responsibility for setting security policy and providing training to promote change in the institutional culture and buy-in among the users. It is appropriate that the CISO function set security policy as the IT function may have differing priorities (for example, convenience and functionality being prioritized over security, yet both are important).

From those who have implemented MDM, benefits cited included less manual efforts and reduced duplication of efforts (for example, configuration profiles are pushed to devices instead of manually configuring devices). Also, MDM provides a way to monitor all enrolled devices to ensure controls are in place (for example, monitoring to ensure devices are encrypted).

Several of the CISOs stated that users at their institutions reported a drain on the battery and other resources on their managed devices. Further testing may be needed to identify whether changes to some of the MDM settings (for example, frequency of check-in) may better conserve battery and other resources on managed devices.

Policies, Procedures, and Documented Guidance

Documented policies and procedures for mobile devices serve to establish guidance for the information security staff and also to make University constituencies aware of expectations and consequences for noncompliance. We compiled a list of topics that we considered appropriate to be addressed by various institutional policies and procedures in regards to mobile devices based on various IT security and auditing sources, such as ISACA (previously known as the Information Systems Audit and Control Association) and NIST. Specifically, we looked for coverage of the following topics:

- Definition of a mobile device;
- Personally-owned mobile devices (Bring Your Own Device or "BYOD");
- Management of sensitive or confidential data;
- Remote access to the network, including acceptable access methods;
- Minimum security configurations (for example, password requirements and encryption);
- Acceptable use of mobile devices;
- Ownership of/access to University data (regardless of device ownership);
- Device disposal and removal of University data;
- Training and user awareness; and
- Disciplinary action for noncompliance.

UT System Policy UTS165, *Information Resources Use and Security Policy*, broadly addresses the protection of information resources and data. It was most recently amended on March 16, 2015 and includes more specific standards to address mobile devices. Specifically, of particular relevance to mobile devices, there are standards that address:

- Information Resources Security Responsibilities and Accountability (Standard 1) – Requires documented permission and justification for any user to store confidential University data on a mobile device.
- Acceptable Use of Information Resources (Standard 2) – The model Acceptable Use Policy (AUP) contains a section covering mobile devices, and institutional AUPs must cover ownership of University data, including those maintained or created on a personally-owned mobile device.
- Malware Prevention (Standard 8) – Personally-owned mobile devices that contain confidential University data must be configured to comply with required University security controls.
- Safeguarding Data (Standard 11) – Institutionally-owned mobile devices must be encrypted, and personally-owned mobile devices must be encrypted if they contain confidential data. Users are responsible for ensuring that University data is backed up to assure access. Also, institutions must discard devices containing University data "in a manner that adequately protects the confidentiality of the data and renders it unrecoverable."

- Server and Device Configuration and Management (Standard 19) – All devices on UT System networks must be protected against malicious attack. Institutional Information Security Officers must establish and communicate minimum security configurations for mobile devices.

While UTS165 is a Systemwide policy applicable to all institutions, most institutions also have their own information security policies. Each institution's constituencies will be most familiar with its own policies, and may not be aware that a relevant Systemwide policy exists. Therefore, because the security of mobile devices is heavily dependent upon user understanding and cooperation, particularly for personally-owned mobile devices, which may not be managed by the institution, we reviewed various institutional policies and procedures (as listed in ***Appendix A***) and summarized our findings below.

We determined that the policies and procedures generally covered the key mobile device topic areas. Particularly, strengths were noted in the areas of (1) management of sensitive or confidential data stored on mobile devices, (2) minimum security configurations, (3) remote access to the institutional network, (4) personally-owned mobile devices, (5) disciplinary action for noncompliance with information security policies, (6) user awareness of mobile device policies and procedures through training and user acknowledgment, and (7) ownership of and access to data residing on mobile devices.

The last item, access to University data residing on mobile devices, is also specifically addressed in the revised UT System model AUP in UTS165 (Standard 2), which clarifies that University data on personally-owned devices are subject to open records requests, subpoenas, court orders, litigation holds, discovery requests, and other requirements as if the data were on a institutionally-owned mobile device.

On the other hand, we did identify opportunities for enhancement across the UT System institutions in the following topic areas:

- *Providing a definition of mobile devices.* Users should be made aware of what constitutes a mobile device at their respective institution and would therefore be covered by applicable policy. While mobile devices are continually developing, NIST provides a good example definition by partially describing mobile devices as those with a "small form factor" and which do not run on "a full-fledged desktop or laptop operating system" (for example, Android and iOS smartphones and tablets, BlackBerrys, connected medical devices, smartwatches, etc.).
- *Disposal of institutionally-managed mobile devices and removal of University data from mobile devices.* Some of the information security staff we interviewed for this audit described their internal procedures for device repurposing or disposal. However, documenting and expanding those procedures would provide clear guidance to information security staff and users, to help ensure that University data are properly managed in a consistent manner in case an institutionally-owned or personally-owned device is lost, stolen, traded, or has reached the end of its useful life. Updated procedures should also provide guidance for users to remove University data from personally-owned mobile devices when the data are no longer needed.
- *Acceptable use of mobile devices.* As mobile devices are becoming more prevalent with users, the acceptable use of these devices should be clearly stated and acknowledged by each user to help deter unwanted behavior and secure information resources. The revised UT System model AUP addresses this item.

  Recommendation (4): The Systemwide Information Security Office should develop additional guidance to assist institutional CISOs with incorporating the revised version of UTS165 into their institutional policies and procedures relating to mobile devices. Part of this guidance should be in

the form of model training materials. Updating policies and procedures and promoting user awareness through a targeted training program should enhance security surrounding mobile devices.

Level (4): This finding is considered **Medium** due to the potential level of information security risk from unclear or insufficient policy guidance.

Management's Response (4): UT System's UTS165, *Information Resources Use and Security Policy* and Standards, was updated this year, and it includes mobile device management requirements (Standards 2: Acceptable Use and 11: Safeguarding Data). Institutions can, and often do, have policies, standards, and procedures that may go above and beyond the requirements of UTS165. The Systemwide Information Security Office will draft a Memorandum to the CISOs highlighting the importance of mobile device management in mitigating risks related to unauthorized exposure of confidential data and enhancing policy compliance and overall information security as well as reminding them of their responsibility to update institutional policy and procedures to incorporate changes in UTS165 related to mobile device management.

The Systemwide Information Security Office will remind institutions of the current availability of the SANS Securing The Human training video regarding mobile device security and will continue the development of a SharePoint site, as part of the UT System CISO SharePoint, dedicated to mobile device management that includes training resources from other UT System institutions, EDUCAUSE, and other institutions of higher education.

Implementation Date (4): August 31st, 2015

We noted that each institution requires users to acknowledge an AUP; however, the institutional AUPs that we reviewed varied in their coverage of topics and their periodic re-acknowledgement requirements were different. Using the revised UTS165, including the UT System model AUP, will promote consistent standards across UT System. Other individual opportunities for enhancement relating to institution-specific policies and procedures, such as areas where policies could be updated and/or expanded, were separately communicated to institutional management.

Mobile Device Inventory

According to the Texas Comptroller of Public Accounts, for accounting purposes, institutionally-owned mobile devices less than $500 are not required to be included in the capital inventory, nor are they required to be tracked as controlled items. While the value of the mobile device itself may be less than $500, loss of the device or unauthorized disclosure of the data on that device could result in consequences exceeding the value of the device. While some institutions have policies requiring lost or stolen mobile devices to be reported, employees may not always do so.

Currently, monitoring of institutionally-owned mobile devices below $500 varies among, and even within, the institutions. According to the CISO staff we surveyed, some institutions' IT departments centrally track all institutionally-owned mobile devices, while other institutions allow each department to decide whether it needs to track its own mobile devices under $500. We advised the institutions that do not centrally track, or have individual departments track, institutionally-owned mobile devices (regardless of dollar amount) to reassess the need and feasibility to do so.

Transition of UT Brownsville (UTB) and UT Pan American (UTPA) to UT Rio Grande Valley (UTRGV)
In March 2015, one interim CISO was appointed to UTB, UTPA, and UTRGV for the transition period. The CISO stated that the immediate priority is to focus on the operational needs of UTRGV (setting up email, computer centers, etc.). Once the fundamentals of ongoing operations have been established, they will begin to consider specific issues such as MDM. However, the CISO did acknowledge that the Acceptable Use Policy (AUP) needs to be brought to everyone's attention.

We understand that the focus on rapid deployment of operational needs at UTRGV is essential to starting a new university, but a strong policy foundation is also important to promote information security awareness among users. Specific policy matters were communicated directly to each institution.

Lessons Learned: Successes and Challenges
Our survey of institutional CISOs revealed that the institutions were at different stages of maturity with respect to mobile device strategies. Our general observation was that the smaller academic institutions tended to have limited mobile device strategies, while the health institutions had more robust programs in place. This difference is partially attributable to the available resources and level of assessed risk at each institution. Throughout our discussions with UT System information security staff, they acknowledged their awareness of the rise in mobile device usage across the institutions and related risks, and described several areas of success and challenge, as described below.

Executive Support and Communication
While a solid policy foundation is important in setting standards and expectations, CISOs also cited executive management support as being critical to the success of implementing mobile device strategy. Executive sponsorship makes project leaders more effective. Together, they must clearly communicate to users the purpose of mobile security policies and MDM to reduce resistance or suspicion. One approach could be to reiterate the need for balance between the convenience of having access to data on mobile devices and giving up some privacy if an employee elects to use their personally-owned device for business purposes. At institutions where MDM has not been implemented yet, informing users in advance could promote buy-in and subsequent compliance.

Administrative and Technical Controls
Institutional CISOs use administrative and technical controls in addition to, or in conjunction with, MDM software to mitigate the risk of mobile devices. Administrative controls include policies and procedures, general information security training, and other communications (e.g., emails and newsletters) that cover mobile device security to some extent and build user awareness. Also, the institutional IT help desks provide support for mobile device issues.

Technical controls include requiring valid credentials for network access, enforcing security policies through ActiveSync, and using apps that do not store data locally on a mobile device. Other information security measures, such as encryption, vulnerability scans, and monitoring outbound emails for certain number patterns, also protect against the accidental disclosure of data. These controls complement each other and can be used with MDM to effectively achieve mobile device security objectives.

CISO Authority and Oversight
Overall, CISOs stated that they have adequate formal authority to enforce mobile device security policies by virtue of their position, and most also believed they had adequate perceived authority from their institutional colleagues (meaning that, regardless of formal authority, employees consider mobile device security policies as mandatory). In limited cases where the CISO thought that employees viewed security

policies as optional, they felt it may be due to cultural differences or mobile device security being a newer topic. Specifically, they said that employees may not understand that the University has an interest in any device used for business purposes, regardless of who owns the device. However, more user awareness through training is expected to remedy this concern.

CISOs reported that instances of noncompliance with policy are met with an appropriate response. In most cases, a reminder from the information security staff to the user who violated a policy is sufficient. However, additional steps may be taken for repeated violations of policy, such as disabling access or reporting the incident to a supervisor. Additionally, we noted that many of the institutions had clear statements indicating that noncompliance with policies is subject to disciplinary action, up to and including termination of employment. This provision is also included in the revised UT System model AUP.

In addition to the information security staff, institutions also reported having various organizational structures that focus on mobile device security, ranging from informal working groups that are convened as needed, to institutional standing committees and regular reporting.

Cloud Storage and Computing

We also inquired of the institutional CISO staff what other aspects of mobile device usage they considered high risks. A majority of the CISOs responded that cloud storage and computing, especially in conjunction with mobile device usage, is a high risk. As of April 2015, some UT System institutions have contracts with certain cloud storage and cloud computing services which have been reviewed for adequate data protection. However, employees may be using cloud services with mobile devices that have not been vetted by UT System information security staff, which represents a challenge.

Like mobile device usage, the use of cloud services and the risks associated with it will increase. The CISOs interviewed during this audit appeared to be cognizant of this issue. Additionally, this topic is being considered in the internal audit function's annual risk assessment process, and audits of cloud services may be planned in upcoming fiscal years.

CONCLUSION

The UT System institutions are currently in various stages of maturity in developing and implementing mobile device management strategies. Based on review of policies and procedures, questionnaire responses, and follow-up meetings, all institutional CISOs are well aware of the emerging use of mobile devices, and corresponding risks, and are evaluating MDM solutions for their respective institutions. We noted opportunities for the Systemwide CISO to improve policy, procedure, and training guidance, which we believe will help reduce risks through increased user awareness and acceptance of each institution's responsibility to protect its data, regardless of where it resides. We also noted an opportunity to reduce the ongoing maintenance cost of the current AirWatch solution by eliminating those licenses not in use.

Appendix A – UT System Institutional Policies Reviewed

We considered the following institutional policies and procedures when assessing the degree of coverage of each mobile device topic. This listing was compiled through a combination of publicly accessible documents on the institutions' websites and inquiring of institutional information security staff. Any institution-specific suggestions for enhancement were communicated to the respective institutions.

Systemwide Policy

1. UTS165 – Information Resources Use and Security Policy, last amended March 16, 2015

UT System Administration

1. INT124 – Information Resources Acceptable Use and Security Policy
2. Information Resources Standards of Operation Manual
   - Encryption Guidelines
   - Management of Confidential Data
   - Recommended Minimals for Employees Personal Computers
   - Remote Network Access
   - Removal, Re-Deployment and Disposal of Equipment and Electronic Media
3. Information Resources Acceptable Use Policy Agreement Form

UT Arlington

1. Computing Device Encryption Requirements
2. Mobile Security
3. Security Standards and Guidelines for Telecommuting or Accessing Restricted Information Resources
4. Policy 5-604 – Information Resources Acceptable Use and Security Policy Agreement
5. Procedure 3-27 – Discipline and Discharge Policy

UT Austin

1. Information Resources Use and Security Policy
2. Protecting Data on Vulnerable Devices (Security Practices Bulletin #1)
3. Acceptable Use Policy
4. Minimum Security Standards for Data Stewardship
5. ISO Wiki on Security Configuration – Approved Encryption Methods for Mobile Devices
6. ISO Wiki on Security Configuration – Handheld Hardening Checklists

UT Brownsville

1. Information Resources Security Operations Manual
2. Minimum Security Standards
3. Policy for the Use and Protection of Information Resources

UT Dallas

1. UTDBP3096 - Information Security and Acceptable Use Policy

UT El Paso

1. Information Resources Usage Policy
2. Acceptable Use Policy
3. Social Security Use and Solicitation
4. Data Classification Standard

5. Laptop/Desktop Encryption Webpage
6. Security Policies

UT Pan American
1. Information Resources Acceptable Use Policy
2. CISO list of policies
3. Computer Encryption Policy
4. UTPA Security Manual

UT Permian Basin
1. Acceptable Use Policy For Information Resources

UT San Antonio
1. 8.12 - Information Resources Use and Security Policy
2. Additional Standards (as referenced in 8.12):
    a. Data Encryption
    b. Disposal of Computing Devices
    c. Information Security Training
    d. Information Security Expectation of Privacy
    e. Network Access
    f. Passwords/Passphrases
    g. Personal Computing Security
    h. Physical Access
    i. Portable Computing Security
    j. Protection Against Malware
3. Standard for Information Resource User
4. Standard for Acceptable Use
5. Standard for Data Encryption
6. Standard for Personal Computing
7. Information Security Incident Response

UT Tyler
1. Information Resources Acceptable Use Policy
2. IT Network Connection Policy
3. Computer Redistribution/Disposal Policy & Procedures
4. iPad/iPhone Security Configurations

UT Southwestern
1. ISR-103: Device and Media Controls
2. ISR-104: Acceptable Use of Information Resources
3. ISR-108: Password Management
4. ISR-110: Network Security Management
5. UHHR 1-101: Use of Portable Electronic Devices – Cell Phones (hospital policy)
6. Privacy Compliance Program Privacy Manual, Policy No: 10.1: Safeguards (for PHI)
7. Mobile & Smartphone Devices setup guidance

UT Medical Branch
1. Information Resources Security Manual (contains an acknowledgement that serves as UTMB's Acceptable Use Policy)

2. IHOP – 02.19.03 – Mobile Communication Devices Policy
3. IHOP – 02.19.06 – Information Resources Security Policy
4. Practice Standard 1.2.8 – Remote Access
5. Practice Standard 1.2.9 – Data Encryption Requirements
6. Practice Standard 14.1.2 – Data Classification
7. Practice Standard 1.19 – Portable Computing
8. Practice Standard 2.1 – Information Security Education & Awareness Program

UTHSC-Houston

1. Policy 180 – Acceptable Use of University Information Resources
2. ITPOL-004 – Access Control Policy
3. ITPOL-025 – Mobile Device Policy
4. ITPOL-031 – Bring Your Own Device (BYOD) Policy
5. Medical and Scientific Device Policy
6. Medical and Scientific Device Standard Operating Procedure
7. Mobile Device Policy Acknowledgement

UTHSC-San Antonio

1. Policy 5.8.7 – Network Access Policy
2. Policy 5.8.10 – Information Resources Acceptable Use and Security Policy
3. Policy 5.8.12 – Portable Computing Policy
4. Information Management Services' MDM Website

UT MD Anderson

1. ADM0334 – Acquisition, Support, and Security of Institutionally-Owned Personal Computers and Mobile Devices Policy
2. ADM0335 – Information Security Office Policy for the Use and Protection of Information Resources
3. ADM1187 – Electronic Confidential and Restricted Confidential Information Access and Storage Policy
4. ADM1188 – Use of Personally-Owned Mobile Devices for Institutional Business Policy
5. Information Resources User Rights and Responsibilities Acknowledgement
6. Information Resources Security Operations Manual

UTHSC-Tyler

1. IHOP 02.04 – Information Resources Acceptable Use Policy
2. IHOP 02.05 – Eradication of Data Stored on Electronic Media
3. IHOP 02.13 – Security Awareness and Training
4. IHOP 02.15 – Malicious Code
5. IHOP 4.5.07 – Storing and Securing PHI
6. IHOP 4.5.09 – Removal of PHI from UTHSCT Facilities

Appendix B – Questionnaire & AirWatch Implementation Status Summary

This table summarizes details from the questionnaire and AirWatch implementation status across UT System. It was prepared using information self-reported by the institutional information security staff.

Institution	Mobile-Related Policies[8]	Personal Devices Allowed[9]	Inventory of Mobile Devices Below $500[10]	Primary MDM Solution[11]	MDM Status/Explanation
UT Arlington	Moderate	Yes	Some	AirWatch & Toggle	Evaluation phase
UT Austin	Moderate	Yes	Some	Absolute Manage	Implemented – Already had a solution; AirWatch not financially attractive
UT Brownsville	Limited	Yes	Yes	None	To be evaluated pending transition to UTRGV
UT Dallas	Good	Yes	Yes	None	ActiveSync controls determined to be sufficient for level of assessed risk
UT El Paso	Good	Yes	No	None	To be evaluated in the near future (insufficient staffing)
UT Pan American	Good	Yes	Yes	MobileIron	To be evaluated pending transition to UTRGV
UT Permian Basin	N/A[12]	Yes	Yes	Meraki	Implemented
UT San Antonio	Moderate	Yes	Per department	Intune	Evaluation phase – Institution to leverage familiarity with Microsoft products; AirWatch not financially attractive
UT Tyler	Moderate	Yes	Per department	AirWatch	Deployment phase (insufficient staffing)
UT Southwestern	Good	Yes	MDM enrolled	AirWatch	Implemented
UT Medical Branch	Moderate	Yes	Some	AirWatch	Deployment phase
UTHSC-Houston	Good	Yes	Per department	AirWatch & Meraki	Deployment phase; Meraki is being deprecated
UTHSC-San Antonio	Good	Yes	Yes	AirWatch	Deployment phase
UT MD Anderson	Good	Yes	Yes	BoxTone & AirWatch	Using BoxTone; beginning to deploy AirWatch
UTHSC-Tyler	Good	Yes	Yes	Absolute Manage	Evaluation phase (insufficient staffing)
UT System Admin	Good	Yes	Yes	AirWatch	Pilot phase

[8] This assessment is a holistic conclusion based solely on mobile device-related topics and the policies reviewed.
[9] Personally-owned mobile device access to an institution's network requires authentication with valid credentials. Otherwise, guest usage provides access to the public Internet only.
[10] Institutionally-owned mobile devices less than $500 are not required to be included in the inventory or to be tracked. However, some institutions have decided to track their own mobile devices under $500.
[11] Many institutions reported using the Microsoft Exchange ActiveSync protocol, in addition to evaluating or using an MDM solution. For simplicity, only MDM products are listed in this summary table.
[12] UTPB did not have institutional policies specifically related to mobile devices. Instead, the institution refers to UT System policy UTS165.