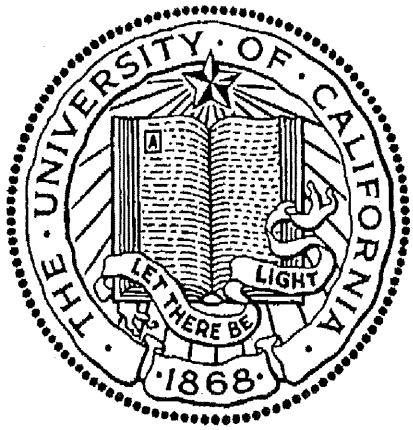

AUDIT AND ADVISORY SERVICES

Information Security – Mobile and Portable Devices Audit
Project No. 14-632

December 15, 2014

Prepared by:

Chad Edwards
Auditor-in-Charge

Reviewed by:

Jaime Jue
Associate Director

Approved by:

Wanda Lynn Riley
Chief Audit Executive

UNIVERSITY OF CALIFORNIA, BERKELEY

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO

SANTA BARBARA • SANTA CRUZ

AUDIT AND ADVISORY SERVICES
Tel: (510) 642-8292

611 UNIVERSITY HALL #1170
BERKELEY, CALIFORNIA 94720-1170

December 15, 2014

Larry Conrad
Associate Vice Chancellor for Information Technology and Chief Information Officer
Office of the Chief Information Officer

Associate Vice Chancellor for Information Technology and Chief Information Officer Conrad:

We have completed our audit of Information Security – Mobile and Portable Devices as per our annual service plan in accordance with the Institute of Internal Auditors' *Standards for the Professional Practice of Internal Auditing* and the University of California Internal Audit Charter.

Our observations with management action plans are expounded upon in the accompanying report. Please destroy all copies of draft reports and related documents. Thank you to the staff of Information Security and Policy for their cooperative efforts throughout the audit process. Please do not hesitate to call on Audit and Advisory Services if we can be of further assistance in this or other matters.

Respectfully reported,

Wanda Lynn Riley
Chief Audit Executive

cc: Executive Vice Chancellor & Provost Claude Steele
Vice Chancellor John Wilton
Interim Chief Information Security Officer Paul Rivers
Senior Vice President and Chief Compliance and Audit Officer Sheryl Vacca
Associate Chancellor Linda Morris Williams
Assistant Vice Chancellor and Controller Delphine Regalia

University of California, Berkeley
Audit and Advisory Services
Information Security – Mobile and Portable Devices

Table of Contents

OVERVIEW

Executive Summary

The overall purpose of the audit was to assess the adequacy of information security controls and practices as required by current campus policy and contemplated by external standards that would be applicable to mobile and portable devices, taking into consideration the campus' open computing environment. For purposes of this audit, we employed a working definition of mobile and portable devices that included laptops, smartphones, and tablets.

The campus has traditionally employed an open philosophy to accessing campus systems. In most instances campus information systems are public facing and a virtual private network (VPN) connection is not required to access campus systems from outside the campus network.

In addition to mobile and portable devices that are purchased by units and managed by departmental or central IT support, the campus allows for faculty, staff, contractors and students to use personally-owned mobile and portable devices to access campus systems and data. Increasingly popular in the private sector, this Bring Your Own Device (BYOD) model offers both benefits and complexity. The BYOD model's benefits include productivity and flexibility with individuals being able to access information while they are away from the campus as well as cost savings since the campus does not have to purchase and manage devices for users with the need for remote access. However, there are also risks with the proliferation of user-owned devices that may not meet the minimum security controls required by policy or that may host malicious software.

We performed a risk assessment to identify and evaluate significant risks to the achievement of information and system security objectives. Based upon the results of our risk assessment, we performed detailed testing in the areas of information security policy and standards, vulnerability scanning and intrusion detection as of May 2014.

With respect to vulnerability scanning and intrusion detection, we observe that the design and execution of current control procedures appear effective.

Information security policy, as applied to devices such as smartphones and tablets, is largely complete and current. We identified opportunities to improve policy requirements for data loss prevention, specifically for encrypting data on mobile devices at rest and sanitizing data that no longer has a business purpose on mobile devices that handle or are used to provide privileged access to other devices processing, storing, or transmitting data classified as protection level one data (e.g., Family Educational Rights and Privacy Act [FERPA] student and personnel records).

We also noted that management has planned actions to improve the overall control environment that affect not only mobile devices but also potentially all devices processing, storing, and transmitting covered data[1] and devices used to provide privileged access to other devices processing, storing, or transmitting covered data. Examples of some of the more important

[1] Data elements with a statutory requirement for notification to affected parties (e.g., Health Insurance Portability and Accountability Act [HIPAA]) and data intended for release on a need-to-know basis (e.g., FERPA student records).

actions, commencing in fiscal year 2015, include implementing the Information Risk Governance Committee, establishing and communicating campus policy to clarify information security roles and responsibilities, and training employees with respect to roles and responsibilities for information security.

Source and Purpose of the Audit

Audit and Advisory Services (A&AS) has completed our audit of Information Security – Mobile and Portable Devices as part of our annual service plan for fiscal year 2014. The overall purpose of the audit was to assess the adequacy of information security controls and practices as required by current campus policy and contemplated by external standards that would be applicable to mobile devices, taking into consideration the campus' open computing environment.

Scope of the Audit

For purposes of this audit, we employed a working definition of mobile and portable devices that included laptops, smartphones, and tablets.

To determine the scope of the audit, we considered the campus' objectives for the security of information stored, processed, or transmitted by mobile devices and the control activities promoted to meet those objectives.

We considered external subject matter guidance and direction issued by the federal government, (e.g., National Institute of Standards and Technology [NIST]) and industry (e.g., Center for Internet Security [CIS]) for managing the security of mobile devices and compared them to our current standards.

We performed a risk assessment to identify and evaluate significant risks to the achievement of information and system security objectives and the means by which the potential likelihood and impact of these risks are mitigated to an acceptable level. The risk assessment covered the extension of internal controls to mobile devices in the following areas:

- governance;
- information security policy and standards;
- communications of objectives and policy;
- data and mobile device ownership and responsibilities;
- data classification guidelines;
- compliance with policy and standards;
- budget;
- risk management;
- information security training;
- vulnerability scanning;
- intrusion detection;
- incident response;
- service requests; and
- security alerts and advisories.

Based on the results of our risk assessment, we selected the following areas for detailed testing: information security policy and standards, vulnerability scanning, and intrusion detection.

Our audit approach included the assessment of the following objectives:

- Campus information security policy and standards that apply to smartphones and tablets are complete and current.[2]
- For vulnerability scanning, the design and operation of scanning procedures were effective for updating the scanning tool to detect new vulnerabilities as they become available and that activities were applied to scan for vulnerabilities in mobile devices on the campus network.
- For intrusion detection, the design and operation of intrusion detection procedures were effective for updating the detection tool to detect attacks or indicators of potential attacks affecting mobile devices.

Our evaluation of information security policy and standards, vulnerability scanning, and intrusion detection controls described above was as of May 2014.

Background Information

The campus has traditionally employed an open philosophy to accessing campus systems. In most instances campus information systems are public facing and a VPN connection is not required to access campus systems from outside the campus network.

In addition to mobile and portable devices that are purchased by units and managed by departmental or central IT support, the campus allows for faculty, staff, contractors, and students to use personally-owned mobile and portable devices to access campus systems and data. Increasingly popular in the private sector, this BYOD model offers both benefits and complexity. The BYOD model's benefits include productivity and flexibility with individuals being able to access information while they are away from the campus as well as cost savings since the campus does not have to purchase and manage devices for users with the need for remote access. However, there are also risks in that there may be a proliferation of user-owned devices that may not meet the minimum security controls required by policy or that may host malicious software.

In addition, with respect to the three areas of focus for our audit testing, we note the following.

Information Security Policy and Standards

The purpose and function of information security policy and standards over mobile devices is to communicate requirements for members of the campus community to protect the confidentiality of information obtained and used in support of campus objectives.

At the time of our audit, key policies and standards created that are applicable to mobile devices include

- Departmental Security Contact Policy;
- Computer Use Policy;
- Minimum Security Standards for Network Devices; and

[2] We used NIST Special Publication 800-124 Guidelines for Managing the Security of Mobile Device in the Enterprise (Souppaya & Scarfone, 2013) and the CIS Benchmarks for Apple iOS (Skrdla, 2013) and Android (Fritz, 2012) as the basis for our comparison to current campus information security policies and standards.

- Minimum Security Standards for Electronic Information.

The IT policy manager, under the direction of the chief information security officer, is responsible for establishing and periodically reassessing policies and standards, including those relevant to mobile devices, whether owned by the campus or individually.

Vulnerability Scanning

The purpose and function of vulnerability scanning, within the context of this audit, is to continually scan for vulnerabilities in mobile devices, analyze the results and remediate legitimate vulnerabilities. The information security operations manager, under the direction of the chief information security officer, is responsible for managing the support and delivery of the campus' network scanning service.

Intrusion Detection

The purpose and function of intrusion detection is to detect attacks or indicators of potential attacks affecting mobile devices. The information security operations manager, under the direction of the chief information security officer, is responsible for managing the support and delivery of the campus' network intrusion detection service.

Summary Conclusion

Overall Internal Control Environment

The campus has embraced the BYOD strategy, which presents both benefits and complexity with securing mobile devices. Some of the benefits include increased productivity, flexibility, and cost savings. The dangers may include

- The proliferation of mobile devices with unknown security risks, because they are not centrally managed as is the case with other devices.
- Smartphones and tablets have weaker security mechanisms than other devices.
- Smartphones and tablets use cloud services more frequently and the cloud services used may not meet campus information security requirements or installed applications may carry malware.

Depending on the circumstances, the consequences may include the unauthorized disclosure, modification, or loss of sensitive information.

Overall, taking into consideration the sometime competing interests of maintaining a generally open campus network, allowing for remote access to campus systems by BYOD devices, and the desire to protect sensitive and confidential data, we identified opportunities to improve the campus control environment with respect to information security that affect not only mobile devices but potentially all devices processing, storing, and transmitting covered data and devices used to provide privileged access to other devices processing, storing, or transmitting covered data.

However, management, prior to this audit, was aware of these opportunities and actions are underway to improve the overall control environment. Examples of some of the more important actions, all of which are commencing in FY 2015, include

- implementing the Information Risk Governance Committee;
- establishing and communicating campus policy to clarify information security roles and responsibilities; and
- training employees in their information security roles and responsibilities under policy.

Although we did not conduct detailed testing of management's proposed actions, in principle they appear appropriate to improve the campus control environment with respect to information security.

Policy

Information security policy applying to smartphones and tablets is largely complete and current. In comparing our information security policies to industry-accepted better practices, we identified opportunities to improve policy requirements for data loss prevention, specifically with respect to encrypting data on mobile devices at rest and sanitizing data that no longer has a business purpose on mobile devices that handle or are used to provide privileged access to other devices processing, storing, or transmitting data classified as protection level one data (e.g., FERPA student and personnel records).

Vulnerability Scanning and Intrusion Detection

Lastly, we observe that the design and execution of control procedures appear effective for

- updating the campus vulnerability scanner to detect new vulnerabilities as they become available and scanning mobile devices for vulnerabilities; and
- updating the capability of the intrusion detection system to detect attacks or indicators of potential attacks affecting mobile devices.

SUMMARY OF OBSERVATIONS & MANAGEMENT RESPONSE AND ACTION PLAN

Mobile Device Policy – Completeness and Currency

Observation

Information security policy as applied to smartphones and tablets is largely complete and current. In comparing our information security policies to industry-accepted better practices, we identified opportunities to improve policy requirements for data loss prevention.

Campus protection level one data is data released on a need-to-know basis. Examples of protection level one data include

- FERPA student records;
- personnel records; and
- data protected or restricted by a contract, grant, or other agreement.

Currently encryption of data at rest is not required by policy for mobile devices processing, storing, or transmitting protection level one data nor for mobile devices used to provide privileged access to devices processing, storing, or transmitting such data.

Based upon our inquiries with management, we understand that management has taken a measured approach to focus primarily on data with greater risk of exposure (protection level two, where there is a statutory notification requirement in case of a breach) and to increase incrementally requirements in campus information security policy. This structured, gradual approach results from concerns about the ability of the campus community to be able to adapt successfully to large changes in information security requirements at one time.

Data sanitization is the process of protecting the confidentiality of data on mobile devices prior to disposing or releasing the device out of the individual's control. In order to comply with our policy, the campus community must (1) use logic techniques that comply with the US Department of Defense (DOD) three-pass method or the Secure Erase[3] method for overwriting data or (2) they must physically destroy the mobile device. Management is currently not requiring data sanitization procedures for mobile devices that may be processing, storing or transmitting protection level one data because currently tools are not available for smartphones and tablets that conform to DOD or Secure Erase methods.

Management therefore has focused its attention on those mobile devices representing a greater risk exposure (listed in decreasing order of risk):

- Mobile devices that provide privileged access to other devices that process, store, or transmit protection level two data.
- Mobile devices that process, store, or transmit protection level two data.

[3] A firmware command, available on certain hard drives, that is used to overwrite completely all data on the hard drive.

- Mobile devices that provide privileged access to other devices that process, store, or transmit protection level one data.

While we agree with management's approach to prioritizing the risk of mobile devices associated with these higher risk activities through policy requirements, we do note that there remains risk associated with the loss or theft of mobile devices with level one data on it, which is not covered by current policy. We believe that the likelihood that protection level one data would be stored on mobile devices used for campus business, whether owned by the university or privately owned by an individual, is non-trivial. Our workforce is increasingly mobile and utilizes such devices for convenience and productivity. We observe an opportunity for management to update campus security policies to require the use of manufacturer alternatives for lower risk protection level one confidential data. While these alternatives, such as a factory reset, do not overwrite the data in a manner contemplated in the DOD standards, they utilize other mechanisms to render encrypted contents cryptographically inaccessible.

Management Response and Action Plan

Controls 15.2 Encryption on mobile devices and removable media and 15.3 Secure deletion upon decommission of the campus policy, Minimum Security Standards for Electronic Information, will be enhanced to change its state from "not required" or "recommended (strongly encouraged best practice)" to a "future requirement" as a part of our annual cycle to incrementally improve security on campus while giving administrative units time to plan for, identify, and make available the resources needed to meet incremental improvements in security. Furthermore, implementing guidance will be revised to specify in the case of mobile device (e.g., smartphones and tablets running iOS and Android) where implementation of this control is more user-friendly and manageable (e.g., in comparison to devices which may or may not be mobile running Microsoft or Apple's latest operating systems). Policy and implementing guidance will be updated no later than July 1, 2015 with an implementation date of July 1, 2016.