Bring Your Own Device:
A Framework for Audit

Emily A Knopp, CPA, CISA
Audit Director
Angelo State University
Member of Texas Tech University System

March 6, 2014

Texas Association of College of University Auditor—2014 Conference

Emily A Knopp, CPA, CISA

- Audit Director for Angelo State University
- Assists is developing and expanding the IT audit activities at Texas Tech University System and its component institutions
- Performs and supervises IT audits across the Texas Tech University System and its component institutions
- Presents at various conferences across higher education

Acknowledgement

Mike Cullen, Senior Manager, CISA, CISSP, CIPP/US
Baker Tilly Virchow Krause, LLP
Baker Tilly Beers & Cutler, PLLC

Objectives

- Briefly define mobile devices and BYOD
- Identify the impact of mobile devices on campus
- Define key mobile device risks and control activities to incorporate into audit work plans
- Describe a audit framework that can be adopted to address the risks and controls specific to mobile devices

Define Mobile & BYOD

Why do we care?

- Mobile is here, no going back to being tethered to a desk
- Mobile allows great productivity and flexibility to achieve institutional objectives
- Mobile employees are happier (so “they” say)
- Mobile can save money (maybe?)

Why is mobile the future?

- A Cisco study says the average number of connected devices per knowledge worker in 2014 will reach 3.3 devices, up from 2.8 in 2012
- Gartner predicts by 2017, half of employers will require employees to supply their own device for work purposes…

BYOE

What are they bringing?

Device	% Own
Laptop	89.1
Smartphone	75.7
Desktop	42.9
Tablet	30.9
Dedicated e-reader	16.2

2013 Almanac, Chronicle of Higher Education

What is a mobile device?

- Any easily portable technology that allows for the storage and transmittal of your organization's sensitive data
- Examples:
  - *Smartphones*
  - *Tablets*
  - *External Hard Drives (e.g., USB thumb drives)*
  - *Laptops*
  - *Cameras (e.g., point and shoot)*
  - *Logistics devices (e.g., GPS Tracking Devices, RFID)*
  - *eReaders*
  - *Digital Music Players (e.g., iPods)*

What is a mobile device?

NIST (SP 800-124) – Characteristics:

- Small form factor
- Wireless network interface for Internet access
- Local built-in (non-removable) data storage
- Operating system that is not a full-fledged desktop/laptop operating system
- Apps available through multiple methods
- Built-in features for synchronizing local data

What is a mobile device?

NIST – Optional characteristics:

- Wireless personal area network interfaces (e.g., wireless networks, Bluetooth, etc.)
- Cellular network interfaces (e.g., 3G, 4G, LTE)
- GPS
- Digital camera
- Microphone
- Support for removable media
- Support for using the device itself as removable storage

What is BYOD?

- Bring Your Own Device
- Higher Ed has been doing this for years
  - *Students, of course*
  - *Faculty, in spite of policies to the contrary*
- Supported by organization systems and applications that allow multiple type of devices to access those services
- Powered by the need for immediate access and freedom from a physical office

BYOD – Pros & Cons

Pros:

- Reduced upfront costs
- Employee satisfaction

Cons:

- Unmanaged devices
- Mingling of personal and institutional data
- Managing legal requirements (e.g., eDiscovery)

Risks and Considerations

Major Security Concerns (NIST)

- Lack of Physical Security Controls
- Use of Untrusted Mobile Devices
- Use of Untrusted Networks
- Use of Apps Created by Unknown Parties
- Interaction with Other Systems
- Use of Untrusted Content
- Use of Location Services

What are the mobile device risks?

NIST Characteristics	Illustrative Risks
Small form factor	Loss or theft of data
Wireless network interface for Internet access	Exposure to untrusted and unsecured networks
Local built-in (non-removable) data storage	Loss or theft of data
Operating system that is not a full-fledged desktop/laptop operating system	Reduced technical controls
Apps available through multiple methods	Exposure to untrusted and malicious apps
Built-in features for synchronizing local data	Interactions with other untrusted and unsecured systems

What are the mobile device risks?

NIST Characteristics	Illustrative Risks
Wireless personal area network interfaces (e.g., Bluetooth, near-field communications)	Exposure to untrusted and unsecured networks
Cellular network interfaces	Exposure to untrusted and unsecured networks
GPS / Location Services	Exposure of private information
Digital camera	Exposure of private information
Microphone	Exposure of private information
Support for removable media	Loss or theft of data
Support for using the device itself as removable storage	Interactions with other untrusted and unsecured systems

Scoping Considerations

- Does your organization have a mobile device strategy, including:
  - *Alignment with institutional strategy/objectives*
  - *Risk assessment(s) for mobility*
  - *Definition of devices*
  - *Policies governing the use of devices (with penalties)*
  - *Security standards based on data*

Scoping Considerations (cont.)

- Who owns these devices?
- Who is responsible for managing and securing the devices?
  - *Recommended basic security*
  - *Incident response procedures*
  - *Antivirus / Antimalware software*
- Who is paying for devices and service plans?
- What are the legal and regulatory requirements for your organization and the jurisdictions you operate in?

Understanding the Institution

- Mission and objectives
- Organization and responsibilities
- Constituents
- Types of data
- Exchanges of data
  - *Interdepartmental*
  - *Third parties*
  - *Interstate or international*
- Data collection, usage, retention, and disclosure
- Systems (e.g., websites, apps)

Identifying Owners and Stakeholders

- Client
- Stakeholders
  - *General Counsel*
  - *Chief Information Officer*
  - *Chief Information Security Officer*
  - *Chief Operations Officer*
  - *Chief Compliance Officer*
  - *Chief Privacy Officer*
  - *Chief Risk Officer*

Assessing Risk

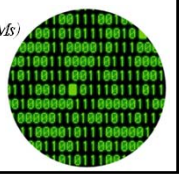
- Leverage management's risk assessments
- Understand the
  - *Regulatory risk*
  - *Legal/contractual risk*
  - *Industry self-regulatory initiatives*
- Consult general counsel
- Public relations

A Framework for Mobile Device Auditing

Mobile Device Framework

Mobile Device Framework – Data

- Data
  - *generated, accessed, modified, transmitted, stored or used electronically by the organization*
  - *essential to the organization's objectives*
  - *requires protection for a variety of reasons, including legal and regulatory requirements*
- Examples:
  - *Messages (e.g., emails, text messages, IMs)*
  - *Voice*
  - *Pictures*
  - *Files (e.g., attachments)*
  - *Hidden (e.g., GPS)*



Mobile Device Framework – Data

- Classification Tiers
- Data Inventory
- Data Owners/Steward
- Authentication & Security Requirements

Mobile Device Framework – Data

- Determine the types of data that can be accessed or stored on mobile devices. Assess restrictions in place to safeguard data.
- Review the Data Classification Security Policy to ensure specificity to the various types of data, based on sensitivity.
- Create an inventory of data, identify the applications and websites where it can be accessed, and determine who will take ownership of the data moving forward.

Mobile Device Framework – Data

- Determine what authentication and security requirements or restrictions are / should be established for each data type.
- Determine if Legal Hold requirements are documented and aligned with data classification and mobile device security.

Mobile Device Framework – Websites & Apps

- Websites and applications require security controls, regardless of the device used for access, to protect the confidentiality, integrity, and availability of data.

Mobile Device Framework – Websites & Apps Examples

Types	Institution	Personal
Websites/Portals	•Email •Intranet/Portal •Financial and HR Systems •Student Information System •Learning Management System	•Google •Yahoo •ESPN
Apps	•Learning Management System •Financial and HR Systems	•Angry Birds •Instagram
Cloud Services	•Google Services •Salesforce.com •Microsoft Office 365	•Gmail •Flickr •Facebook
App Stores	•Apple App Store •Google marketplace •Amazon App Store •Custom Corporate Stores	•Apple App Store •Google marketplace •Amazon App Store
Virtual Desktop Environments	•Citrix •VMware	•GoToMyPC •VNC

Mobile Device Framework – Websites & Apps

- Determine the websites and applications that are used on mobile devices to access data, and determine whether they are approved.
- Assess how the websites and applications are secured to protect data.
- Review all applications and websites accessible via mobile devices to ensure they comply with security policies (e.g., encryption requirements, storage restrictions, access permissions).

Mobile Device Framework – Devices

- Devices require an increasing variety of security controls due to the increased mobility, choice, functionality, and replacement of these products.
- Institution vs. Employee Owned
- Managed vs. Unmanaged

Mobile Device Framework – Devices

- Encryption
- Data transfers (e.g., sending and syncing)
- Logical security (e.g., linkage to HR, passwords, access management)
- Physical security
- Network Architecture (e.g., configuration, monitoring)
- Mobile Device Management

Mobile Device Framework – Devices

- Assess how mobile devices are secured to protect data.
- Determine the types of mobiles devices that are used to access data and whether each mobile device is supported by the institution.
- Ensure that both institutionally-owned and personally-owned mobile devices that access confidential data are secured with appropriate security controls.

Mobile Device Framework – People

- People require frequent communications and trainings on the risks, adopted policies, best practices, and tools for protecting the confidentiality, integrity, and availability of data.

Mobile Device Framework – People

- Organization-wide Mobile Device Policy
  - *Based on the Institution's strategy for mobile devices*
- Policies and Procedures
- Training and Awareness Programs
  - *Content*
  - *Communication*
- Acknowledged Roles and Responsibilities
  - *BYOD Agreement*
- Monitoring

Mobile Device Framework – People

- Determine who uses mobile devices to access data, and who supports and manages those mobile devices that access data.
- Assess training and awareness programs that inform mobile device users of the risks involved and their personal responsibilities when accessing information.
  - *What is the responsibility of the employees?*
  - *Does the content align with adopted policies and procedures?*
  - *Are employees okay with the institution wiping their device?*
  - *What happens to the personal data on the device?*

Mobile Device Framework – People

Additional Considerations:

- Labor laws (exempt v. non-exempt; overtime)
- Tax laws (reimbursement for services, devices)
- Export Control laws
- Record Management laws
- Local Jurisdiction laws

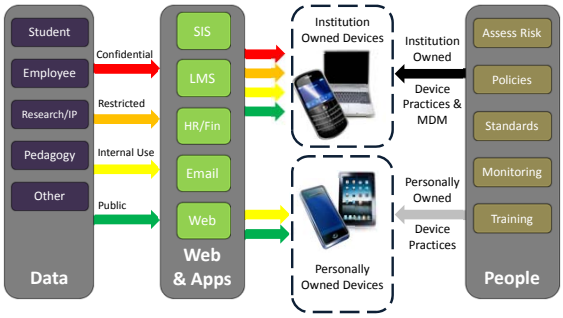
Mobile Device Framework – Policy Considerations

- Determine if an overarching Mobile Device Security Policy exists.
  - Flexible across all platforms and devices
  - Covers basic security measures such as
    - *Passcodes*
    - *Auto-lock*
    - *Local memory wipe*
    - *Wi-Fi settings*
    - *Antivirus / Antimalware*

Mobile Device Framework – Policy Considerations

- Assess existing policies and procedures that guide the procurement, use, support, and management of mobile devices.
- In addition to a mobile device policy, other institutional policies also need to address the use of mobile devices:
  - *Acceptable Use*
  - *Data Classification*
  - *Antivirus/Antimalware*
  - *Security Incident Response*
  - *Business Continuity*

Mobile Device Framework – Sample



Major Security Concerns (NIST) – Mapped to Framework Area

Security Concern	Data	Websites & Apps	Devices	People
Physical Security Controls			X	X
Untrusted Mobile Devices			X	X
Untrusted Networks			X	X
Untrusted Apps	X	X		X
Interaction w/ Other Systems	X	X	X	X
Untrusted Content	X	X		X
Unprotected Data Storage	X	X	X	X
Location Services	X	X	X	X

Angelo State's Approach

- BYOD, unmanaged environment
- First & Foremost – PROTECT THE DATA
  - *Authentication and Authorization*
  - *Secure transport (e.g., SSL)*
- Developing policies and procedures
- Network designed to mitigate risk of running out of IPs
  - *Most students and staff have 3 to 4 devices on the network at any given time.*

Resources

ISACA Mobile Computing Security Audit/Assurance Program

What is it?	• Work program to execute a controls review of mobile computing • Focused in two areas: planning and scoping, security • Also includes a framework for control maturity assessment`
How to use it?	• Use as a base work program to conduct a controls review of your mobile device environment
Challenges to IA	• Access to data… how to audit personal devices • More policy controls over technical controls
Publisher	• ISACA (http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Mobile-Computing-Security-Audit-Assurance-Program.aspx)

Resources

- National Institute of Standards and Technology, Special Publication 800-124 Revision 1 (Final), Guidelines for Managing and Securing Mobile Devices in the Enterprise, June 2013
- National Institute of Standards and Technology, Special Publication 800-144, Guidelines on Security and Privacy in Public Cloud Computing, December 2011
- Digital Services Advisory Group and Federal Chief Information Officers Council, Bring Your Own Device, A Toolkit to Support Federal Agencies Implementing Bring Your Own Device (BYOD) Programs, August 2012

QUESTIONS??

Contact Info

Emily A Knopp
emily.knopp@angelo.edu
325-942-2261

THANK YOU!