Los Angeles Digital Government Summit

Mobile Security and BYOD

L.A. Hotel Downtown (formerly known as L.A. Marriott Downtown)
Wednesday September 26, 2012
10:45 am – noon

Robert Pittman Jr., M.P.A., CISM
Chief Information Security Officer
County of Los Angeles

Factoids

- Nearly 90% of security IT managers strongly or somewhat strongly agree that mobile devices are equal endpoints in the enterprise and want to secure and manage them on par with desktops and laptops
- Top three mobile security practice "must haves"
  - Protecting information on devices (90%)
  - Authentication to the network and apps (89%)
  - Setting and maintaining security policies (88%)

Source: 2011 IDG/CSO Quick Poll (survey of 124 qualified respondents)

The Strategy

- ✓ Adopt portable device / BYOD IT security policy
- ✓ Establish security and privacy minimum requirements
- ✓ Select Mobile Device Management (MDM) solution
- ✓ Manage public online storage sites (e.g., Dropbox)
- ✓ Embrace Encryption (i.e., “Safe Haven”)
- ✓ Enhance Authentication
- ✓ Enhance Authorization

Los Angeles Digital Government Summit

Data Classification Standard

Data Types Used on Smartphone		Smartphone Manufacturers Recommended							
		Apple iOS	Google Android	RIM BlackBerry	MS Windows Mobile 7	Apple iOS	Google Android	RIM BlackBerry	MS Windows Mobile
		Employee Purchased				County Purchased			
1	Legislative sanctioned (e.g., HIPAA/HITECH, WIC)	NS	NS	NS	NS	S	NS	S	NS
2	Confidential / Sensitive	S	NS	S	NS	S	NS	S	S
3	Non-Confidential / Non-Sensitive	S	S	S	S	S	S	S	S

Los Angeles Digital Government Summit

Data Classification Standard (2)

Mandatory Requirements		SMARTPHONES (Manufacturer and their Operating System)				
		Apple		Google Android	RIM BlackBerry	MS Windows Mobile 7
		iOS 3	iOS 4			
1	Anti-virus software (recommended)	S	S	S	S	S
2	Autolock capability (30 minutes maximum)	S	S	S	S	S
3	Bluetooth discovery disabled	S	S	S	S	S
4	Password login to unlock the device	S	S	S	S	S
5	Remote Wipe (restore to Factory default)	S	S	S	S	S

Guidelines

- ✓ Understanding on the capabilities of “Remote Wipe”
- ✓ Identify your MDM solution: sandboxing or traditional
- ✓ Examine if management of apps is necessary
- ✓ Policy management (e.g., lock & wipe, block YouTube)
- ✓ Corporate / Personal data (e.g., Email, docs, apps)
- ✓ Security compliance (e.g., detects Jailbreak, encryption)
- ✓ Enterprise scalable (e.g., mail server integration, multi-tenancy, tiered administration)

Los Angeles Digital Government Summit

Thanks for your attention!

Questions?