Mobile Devices: BYOD

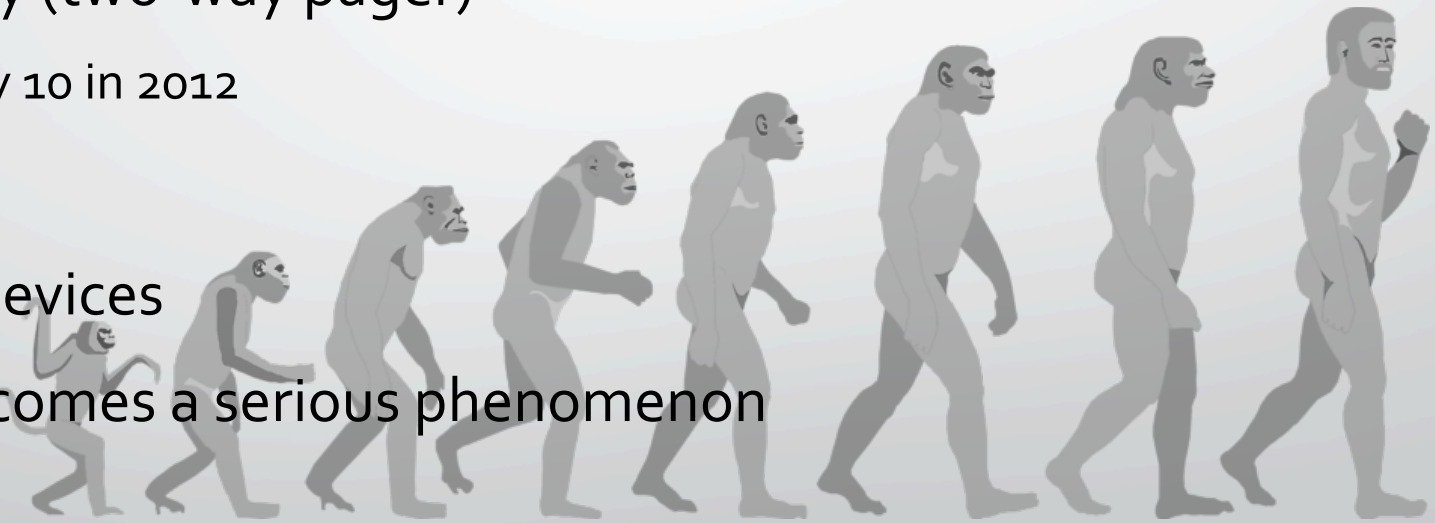
Start Secure to stay Secure

Introduction

- 30+ Years IT Experience
- UNCLE CU Board Secretary
- Cyber Security Analyst at LLNL
  - CSP New Technology Lead
  - Mobility is my passion - secure ubiquitous access (any time, any device, any place)
- I like to keep things interactive

History

- 1997: Palm Pilot (PDA)
  - Palm Treo (Windows Phone 6) 2008
  - HP Web OS in 2009
- 1999: Blackberry (two-way pager)
  - Blackberry 10 in 2012
- 2007: iPhone
- 2008: Android devices
- 2012: BYOD becomes a serious phenomenon



Drivers towards BYOD

- iPhone *plus* Android:
  - was "Blackberry vs. Palm"
  - Real productivity from a mobile device
- Increased faster connectivity:
  - Cellular data—3G, 4G, LTE—pervasive
  - Voice (phone) secondary
- Always working, always connected

Options for Workspace Mobility

- COBO – Corporate-Owned Business-Only
  - Device managed like any corporate asset
  - Tight controls
- COPE – Corporate-Owned Personally Enabled
  - Still corporate asset
  - Allow for use with personal email, apps
- BYOD – Bring Your Own Device (or Disaster)
  - My device can also do corporate things?

Management Sees Risks

Enterprise Mobility Management

Corporate Practices

- Updated incident response plan, to include:
  - E-discovery
  - Forensic access
- Appropriate user agreement that users really follow
- Compensation and recognition, including:
  - Cost model
  - App purchases
  - License management
    - Reclamation of idle apps
    - Rapid access to corporate apps
- Awareness and training

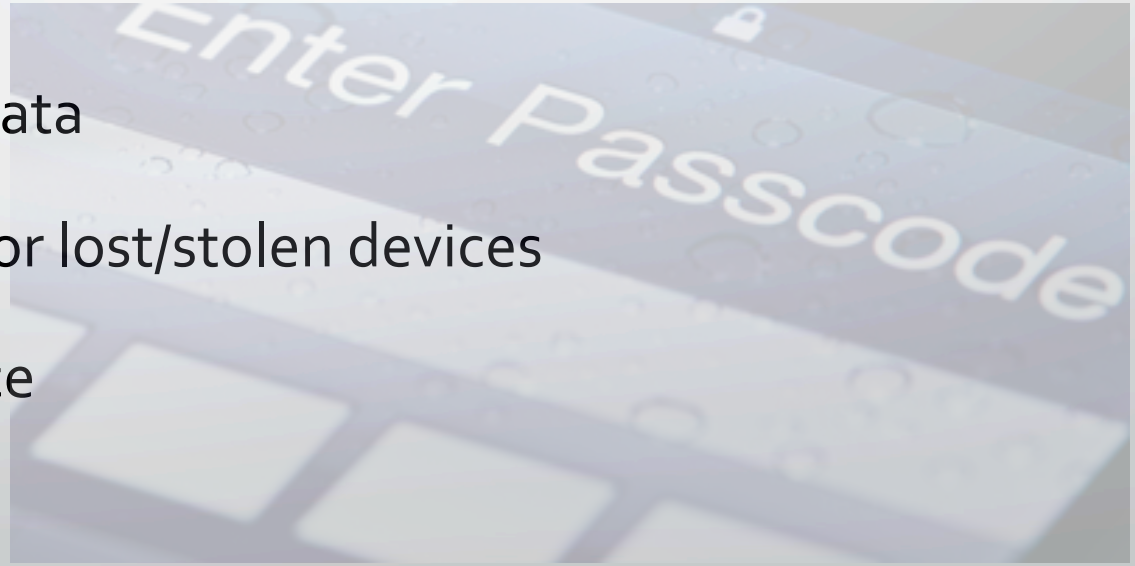
User Counterpoint

User Counterpoint (cont.)

- Added (non-reimbursed) Costs:
  - More capable device
  - More data/voice plan
- Expected response time:
  - On-call
  - Labor laws
- Why carry more than one device?
- If unwilling to BYOD will it count against them?

Minimum Standards

- Encrypt corporate data on device
- Password to access corporate data (commensurate with corporate access controls)
- Password on device
- Remote wipe of corporate data
- Remote wipe and tracking for lost/stolen devices
- Root/jailbreak zero-tolerance



Minimum Standards (cont.)

- Container or full device
- Tethering/hot spot
- Connection to corporate IT or network
- Hardware and software updates
- Other limitations on use:
  - Restrictions on capture/recording
  - Conducting outside business
  - Illegal or illicit activities

Tools

- Mobile Device Management (MDM)
  - Manages entire device
  - May be too heavy-handed for BYOD
- Mobile Application Management (MAM)
  - Manages applications rather than device:
    - Addresses privacy and control concerns
  - Understand MAM's limitations:
    - Can you have corporate and user versions of apps?
    - Risks of per-application VPNs

Conclusion

- BYOD needs to be accommodated.
- Both sides must work together to balance risk/reward.
- Review implementation and adjust:
  - Experience refines understanding of needs
  - Technology evolves rapidly
- Start secure from the get-go, not adding on later.
- White Paper: https://www.sans.org/reading-room/whitepapers/analyst/enabling-large-scale-mobility-security-ground-35847