



Office of the Chief Information Officer

April 25, 2013

# BYOD and Mobile Device Management



Scott Bream  
Office of the CIO  
[scott.bream@ofm.wa.gov](mailto:scott.bream@ofm.wa.gov)

# Topics to be covered

- What is Bring Your Own Device?(BYOD)
- What is Mobile Device Management?(MDM)
  - Policy
  - Tools
- What we currently have and where we are going

# What is BYOD?

- Kind of like BYOB, but not as much fun
- The phenomenon whereby employees bring their own devices to work and use them to conduct company business.
- Cisco Systems released a report earlier this year saying 42% of knowledge workers own the smartphones they use for work, and two-thirds of companies expect this trend to increase.
- The results can be somewhat like BYOB!

# What kind of devices are we talking about?

- A portable device with wireless network and/or cellular communications capability and cellular service plan, such as a cell phone, smart phone, data card, cellular-enabled tablet, or any other such type device.
- You know one when you see one!

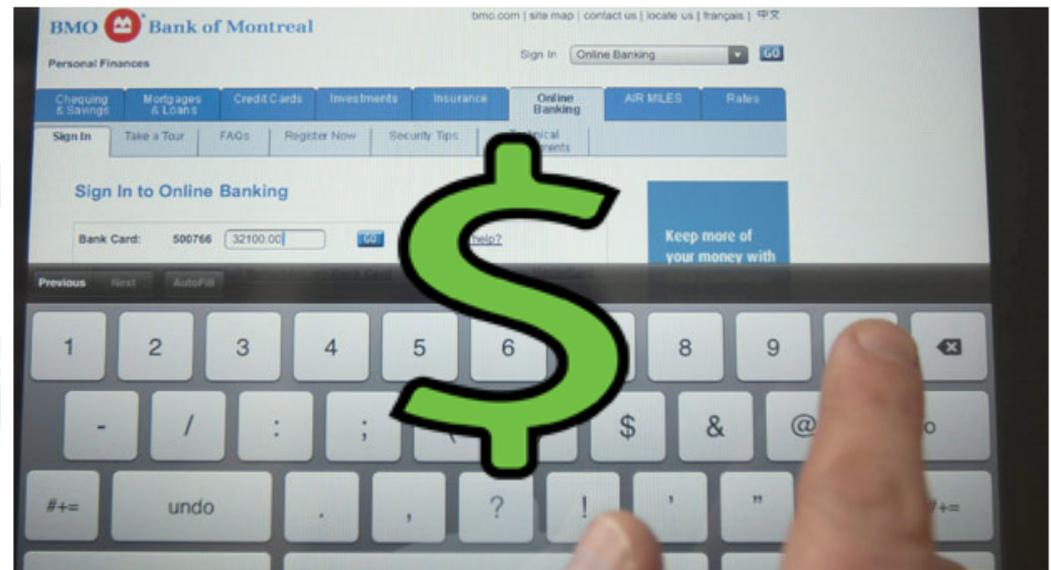


# BYOD

## They may be small, but they are very powerful!

### Hackers moving to target mobile devices, security firm says

CBC News | Posted: Jan 3, 2012 1:31 PM ET | Last Updated: Jan 4, 2012 5:18 PM ET 79



Cybercriminals are moving away from hacking into personal computers to attack personal mobile devices, says a new study of the top cyber threats for 2012. (Ryan Remiorz/Canadian Press)

- Facebook 45
- Twitter 35
- Share 80

As cybercriminals improve their toolkits and malware, they're moving away from hacking personal computers to mobile devices, as well as plotting other more sophisticated attacks, according to a report on the top cyber threats for 2012.

# Why do people bring their own devices?

- They are already in their purse or pocket
- It's how they interface with the rest of world – why should work be any different?
- Its more convenient – why carry multiple devices?
- De Minimis use no longer an issue
- They're better than what the state gives them!
- *They* believe they can be more productive using them

# Why would the State encourage BYOD?

- It's inevitable
- Shifts cost to the user
  - User pays for device, manages and pays cell plan, automatically “upgrades” to the latest and greatest
  - Provider responsible for fielding technical support calls, maintenance and repair
- It empowers the employee to be more productive – and this is important!

# What is Mobile Device Management?

- It's what we do in response to BYOD
- It is evolving
- It's really about managing the *data*, and not the device
- Primarily a two-pronged approach:
  - Policy
  - Tools

## OCIO Policy No. 191

Addresses management and controls relating to use of state-owned and personal cellular devices

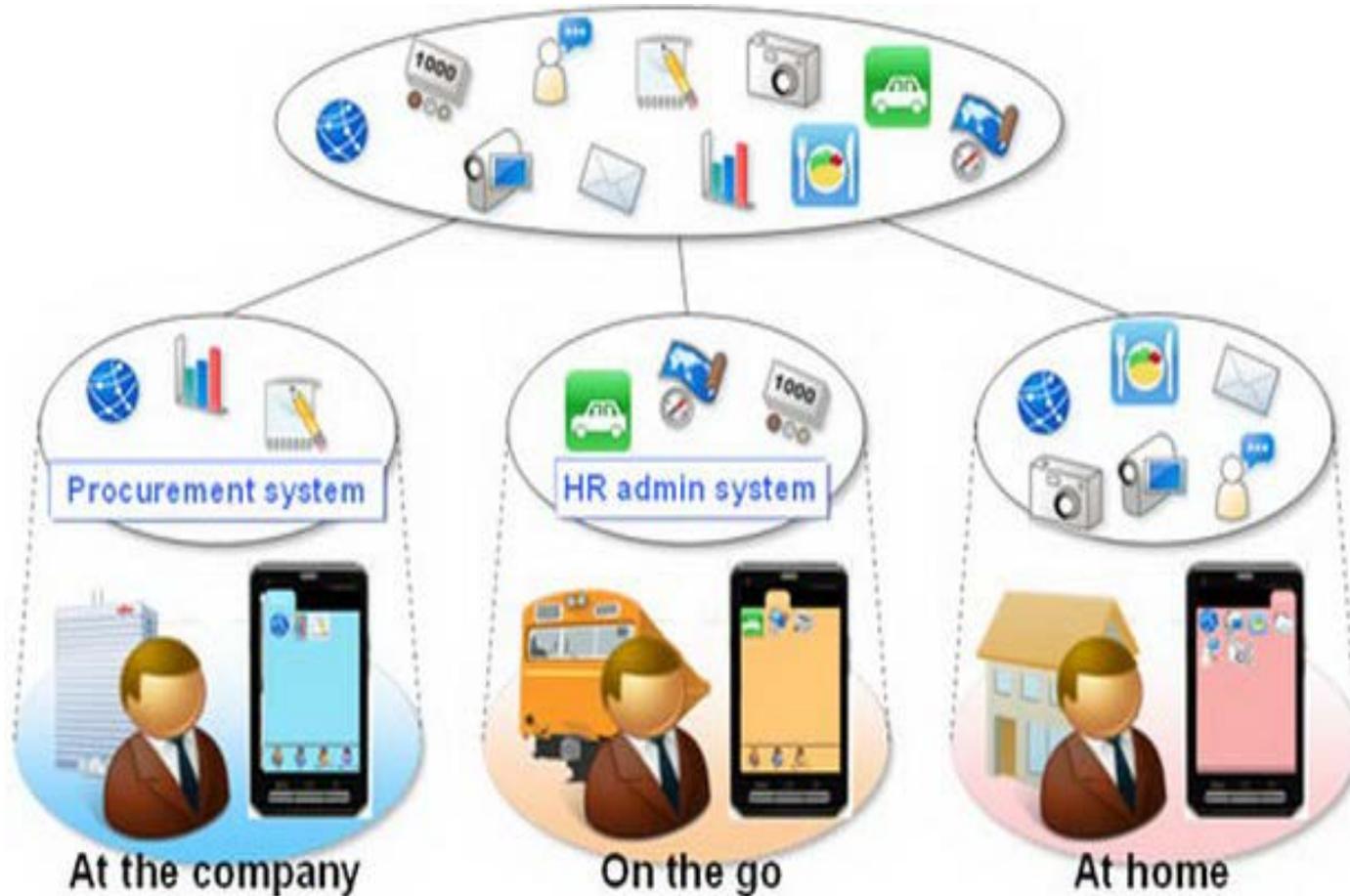
- State-owned devices
  - Conditions that allow for issuance of a device (based on job requirements)
  - Work with DES to get best rates and plans
  - Security and records-retention requirements

- Personally-owned devices:
  - Conditions that allow for use (based on job requirements)
  - Allowance for monthly stipends
    - Voice access - \$10.00/month
    - Data access - \$30.00/month
    - Voice and Data - \$40.00/month
  - Employee is responsible for purchasing device, maintaining service plan and paying monthly bill
  - Employee is responsible for maintenance of device

# So what's the big deal?

- In a word – DATA!
- As stewards of the citizen's data, we must always be asking two questions:
  - Where is the data?
  - Do I have control over it?
- It may be your device, but its my data (some of it, anyway...)

# So what's the big deal?

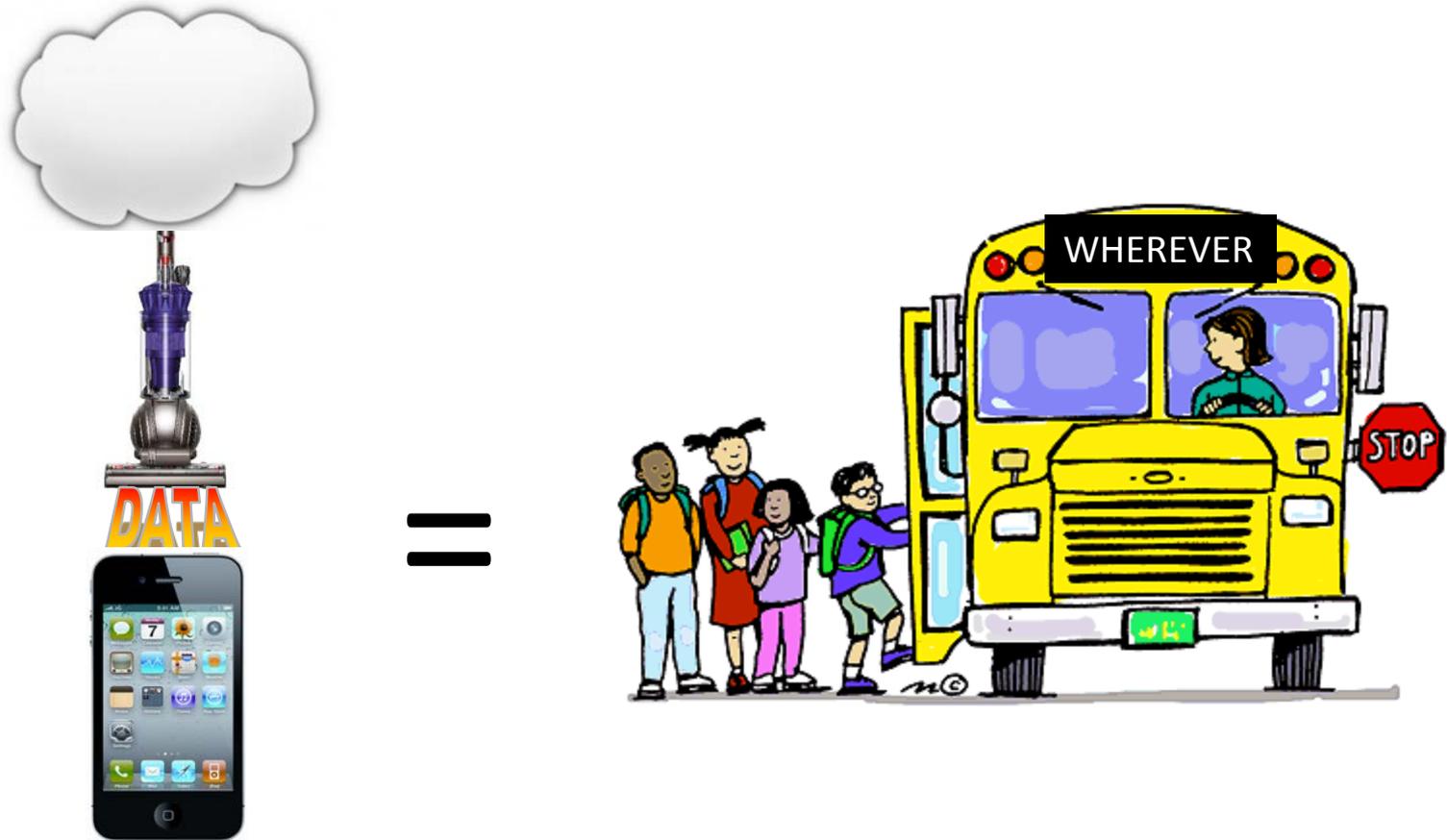


# The Problem with Mobility

\$2.5 Billion Worth of Smartphones Stolen Every Year!



# Cloud-based Backup Services



# Cellular Device Policy – the “Yeah, buts” ...

- All employees who use a personal cellular device to access business documents and communications must comply with statewide and agency-specific security standards, records management and retention schedules...
- All call records, documents and data, photos, etc. used to conduct state business, and made via personally-owned devices, are subject to records retention requirements and public records disclosure.
- Personal call records and other information (e.g. personal data, photos, text messages, etc.) may be subject to review or audit in the event of a litigation hold or public disclosure request.
- The owner of a personal cellular device may be required to surrender the device, including all personal and business related information, if it is subject to a public records request or litigation hold.
- If the device is lost or stolen... the cellular device will be subject to being wiped remotely
- Employee must complete **Cellular Device Authorization and Agreement**

## Phase 1 – CTS ActiveSynch

- A Microsoft client that pushes Outlook content (e-mail, calendaring) from the state Exchange server to your phone
- Ability to enforce timeout thresholds, use of encryption and other security controls
- Mandatory controls
  - Must use PIN that locks entire device
  - Maximum number of failed login attempts before device is wiped remotely
  - Ability to remotely wipe the device if lost or stolen
- Manages the *entire device*

## Phase 2 – Deploy Enterprise MDM Solution(s)

- Provisioning
- Policy enforcement
- Asset management
- Administration
- Reporting

## Product Differentiators

- On-premises vs. cloud-based
- Containerization
- Mobile Application Management (MAM)
- Enterprise Content Management

# Next Steps

- CTS issued a RFI for MDM solutions in September 2012
  - ~ 15 responses received
- CTS plans to issue MDM RFP early May
  - will select one or more MDM providers

# Questions?

# Thank You

Scott Bream, OCIO  
scott.bream@ofm.wa.gov