Mobile Device Management Service: Helping Ministries Mitigate Mobility Risk

OCIO Security Day

November 2016

BRITISH COLUMBIA

OCIO

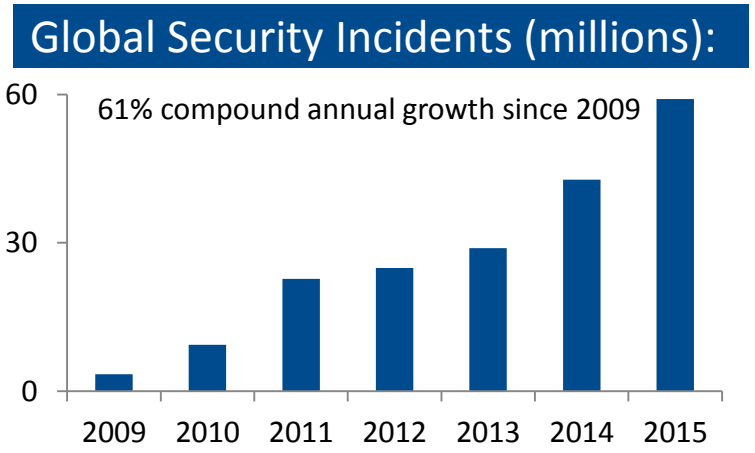
Office of the Chief Information Officer

Agenda

- Mobile Security Context
- Mobility Security Audit
- Helping Government Manage its Mobility Risk
- User Considerations
- Questions

Mobile Security Context

- 12,000 new and unique mobile malware problems are detected every day
- Android devices are targeted by 97% of malicious mobile software
- Ransomware for mobile devices is rapidly increasing
- Cyber attacks are more:
  - frequent
  - effective
  - targeted
  - profitable
  - sophisticated



Mobility Security Audit

- Audits are opportunities to take stock of your current environment and to look for improvements
- They remind us of the risks with the “mini-computers” in our hands.
- If government devices aren’t well managed and secure we all run the risk of:
  - Exposure of citizens’ confidential information
  - Economic harm to government
  - Loss of confidence in government
- Full audit can be found at the http://www.bcauditor.com/

Helping Government Manage its Mobility Risk

- Mobile Device Management Service provides ministries with the tools they need to meet their security and policy obligations. It provides enhanced security capabilities such as:
  - only government approved devices and employees get access
  - no more downloading apps from unknown sources
  - standardised device lock-out time
  - access to Anti-virus
- Offers Ministries real-time:
  - asset management capabilities
  - access to an Admin Console with the ability to wipe lost and stolen devices
  - insight into the applications downloaded onto corporate devices
  - access to your own catalogues where you can put approved business apps

User Considerations

- Enrollment in the new MDMS service is mandatory for all mobile devices, including smartphones and tablets
- Increased visibility of the mobile applications downloaded onto corporate devices
  - Users are notified of this change in their invite emails and have been encouraged to “spring clean” their devices
- Users are still required to follow corporate policy for downloading business and/or personal apps on devices
- Service was launched on July 12, 2016
- Target date to complete migration of all devices - Dec 31, 2016

OCIO will continue to:

- Update mobility standards by March 2017
- Notify ministries if we become aware of malicious apps
- Notify ministries when their devices are non-compliant and need remediation
- Monitor and log device activities
- Continue to enhance security awareness programs

Working together, we can reduce risk and do our part to secure government information.

Questions

OAG Mobility Audit

- Seven recommendations were made for government including these four.
  1. provide ministries the ability to maintain a detailed inventory of all mobile devices
  2. ensure additional security settings are applied before a mobile device goes into service
  3. enforce a maximum inactivity-until-locked time through technical means
  4. replace the existing mobile device management tool with one capable of installing and maintaining anti-malware software, preventing unauthorized mobile devices from connecting, and monitoring and logging mobile device security incidents assessment of risks associated with new mobile device features and services