Mauritian Computer Emergency Response Team

Enhancing Cyber Security in Mauritius

Guideline on Mobile Devices Security (Updated)

National Computer Board
Mauritius

Version 2.0
**DISCLAIMER:** This guideline is provided “as is” for informational purposes only. Information in this document, including references, is subject to change without notice. The products mentioned herein are the trademarks of their respective owners.
## Table of Contents

1.0 Introduction .......................................................................................................................... 4  
1.1 Purpose and Scope ............................................................................................................. 4  
1.2 Audience ............................................................................................................................ 4  
1.3 Document Structure .......................................................................................................... 4  
2.0 Background .......................................................................................................................... 5  
2.1 The Major Smartphone Operating System Complete Comparison .............................. 5  
3.0 Mobile Role-based Methodology ...................................................................................... 19  
4.0 Mobile Platforms Ratings .................................................................................................. 21  
4.1 Apple iOS .......................................................................................................................... 22  
4.2 Android ............................................................................................................................. 22  
4.3 Blackberry OS .................................................................................................................... 22  
4.4 Windows Phone ................................................................................................................ 22  
5.0 The Security Posture of Major Mobile Operating Systems ............................................. 24  
5.1 BlackBerry OS .................................................................................................................. 24  
5.2 Apple iOS .......................................................................................................................... 28  
5.3 Google Android ................................................................................................................ 25  
5.4 Microsoft Windows Phone .............................................................................................. 28  
6.0 Conclusion ......................................................................................................................... 31  
7.0 References .......................................................................................................................... 32
1.0 Introduction

1.1 Purpose and Scope

The previous guideline offered an insight into the risks associated with mobile devices and provided the countermeasures available to minimise them. This guideline had been updated, keeping in mind that technology keeps getting sophisticated and hence risks keep on changing. The aim of this document is to provide a clear demarcation of the different mobile operating systems available, their shortcomings and their security posture when connected into the working environment.

1.2 Audience

This document, while technical in nature, provides the background information to help readers understand the topics that are discussed. The intended audience for this document include users of mobile devices, security professionals, IT managers, system and network administrators involved in the support of mobile devices.

1.3 Document Structure

This document is organised into the following sections:

Section 1 provides a brief overview of the document’s content.
Section 2 gives a background on mobile devices and BYOD.
Section 3 presents the security concerns associated with mobile devices.
Section 4 elaborates on the countermeasures available to mitigate the risks, threats and vulnerabilities discussed in the previous section.
Section 5 concludes the document.
Section 6 contains a list of references used in drafting this document.
2.0 Background

Mobile devices such as smartphones and tablets are a must nowadays. They are generally small and have a variety of attractive functionalities, including sending and receiving e-mails, storing documents, delivering presentations, and remotely accessing data. These devices are useful to practically everyone; however, they also pose security risks to organisations as well as everyday users.

An increasing number of companies are opening corporate networks and data to consumer mobile technology. The resulting trend, usually referred as the consumerization of enterprise mobility, assumes even more disruptive connotations when the employees are allowed to use their own smartphones and tablets to work - commonly referred as BYOD or Bring Your Own Device.

Consumer technology is convenient, easy to learn, and fun to use. However, consumer technology is generally not as secure and manageable as required by the enterprise. Consumer technology brings real business value in terms of productivity and business agility. However, the lack of a strategic approach to the consumerization of IT creates security risks, financial exposure, and a management nightmare. Rather than resist it, organizations should embrace consumerization to unlock its business potential. This requires a strategic approach, flexible policies, and appropriate security and management tools.

A strategic approach to consumerization starts with a clear understanding of the security and management capabilities of each mobile platform. While no mobile platform is immune from security vulnerabilities and management limitations, some platforms are more mature than others with regard to supporting the most appropriate set of policies required by the different mobile roles within the organization.

2.1 The Major Smartphone Operating System Complete Comparison

Individual employees carry along mobile devices into the enterprise, contrary to desktop computers. The tables on the following pages show the comparison between the major OSs which are dominating the smartphone market today, these are namely iPhone iOS, Android, Blackberry OS and Windows Phone 8.
# Media & Gaming

## Web Browsing

<table>
<thead>
<tr>
<th>Platform</th>
<th>Browsing</th>
</tr>
</thead>
</table>
| iPhone iOS 6.1 | Excellent browsing experience  
Reader feature shows just article text, removing clutter and reducing data use  
Full screen browsing, tab syncing over iCloud |
| Android 4.2 Jelly Bean | Google Chrome gives a fast and excellent browsing experience  
Browsing can be synced across phone and desktops  
Default browser can be changed |
| Blackberry OS 10 | No longer supports Adobe Flash (Adobe is abandoning mobile Flash anyway), though it can be enabled with some tech expertise |
| Windows Phone 8 | Excellent browsing experience, full HTML5 browser  
Internet Explorer 10 compresses web pages to reduce your data usage  
Search hotkey cannot be linked to Google  
Many websites don't run well on Internet Explorer 10 |

## Camera & Photos

<table>
<thead>
<tr>
<th>Platform</th>
<th>Quality</th>
<th>Apps</th>
<th>Features</th>
</tr>
</thead>
</table>
| iPhone iOS 6.1 | Excellent quality, lots of apps to enhance the experience  
Physical shutter release button, take photos from lock screen  
Rapid shooting  
Shared Photo Streams easily shares photos between multiple devices and desktops |
| Android 4.2 Jelly Bean | Settings menu pops up wherever you tap  
Very good quality, cool features like panorama shots, time-lapse films  
Excellent photo editing features  
Automatic, unlimited photouploads to Google+  
No shutter lag, rapid shooting |
| Blackberry OS 10 | Time shift feature allows you to rewind or fast forward certain sections of your photo, to capture the perfect moment  
Good editing and effects suite for videos  
Story Maker can quickly make a fun slideshow combining photos and videos  
Physical camera button |
| Windows Phone 8 | 'Lens' feature lets you select from 3rd-party filters to customize your camera  
Physical camera buttons  
Nokia handsets tend to have excellent cameras  
Auto-fix option improves photo quality  
Text recognition in photos with Bing Vision  
Can't upload videos to YouTube easily |

---
<table>
<thead>
<tr>
<th>MUSIC &amp; VIDEO</th>
<th>MUSIC &amp; VIDEO</th>
<th>MUSIC &amp; VIDEO</th>
<th>MUSIC &amp; VIDEO</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Player</strong></td>
<td><strong>Player</strong></td>
<td><strong>Player</strong></td>
<td><strong>Player</strong></td>
</tr>
<tr>
<td>Excellent for music with its iPod influences</td>
<td>Google Music is not intuitive to use, with inconsistent menus and layouts from screen to screen</td>
<td>Songs bought from the Music store are automatically stored on the cloud and available across your Microsoft devices</td>
<td>Music player and management need improving - no direct navigating to a specific place in a song, difficult to manage playlists</td>
</tr>
<tr>
<td>iTunes gives you access to a huge library of apps, movies, tv, music, and books</td>
<td>Support many music and video file formats</td>
<td>No native Podcast app (Nobex looks promising)</td>
<td>No gapless playback</td>
</tr>
<tr>
<td>Few file formats supported natively</td>
<td>Google Music adds up to 20,000 songs that you own, and makes them playable anywhere for free</td>
<td>Large selection of music, TV and movies, though they seem pricier than on other stores</td>
<td>No Podcast management is poor</td>
</tr>
<tr>
<td>Dedicated Podcasts app with iCloud sync</td>
<td>Automatically generate playlists based on recently played songs</td>
<td>Easy streaming to DLNA players e.g. PS3, DLNA TVs</td>
<td>No Wi-Fi syncing to podcasts on a PC</td>
</tr>
<tr>
<td>iTunes Match scans the music you have in your desktop and makes it available online to your Apple devices for a fee</td>
<td>Some handhelds have Beats Audio technology for improved headphone sound</td>
<td>Some handhelds have Beats Audio technology for improved headphone sound</td>
<td>No Wi-Fi syncing to podcasts on a PC</td>
</tr>
<tr>
<td>Easy streaming of media via Airplay to Airport Express, Apple TV, etc</td>
<td>Share fully playable songs with friends via Google+</td>
<td>Share fully playable songs with friends via Google+</td>
<td></td>
</tr>
</tbody>
</table>
## Hardware

<table>
<thead>
<tr>
<th>Handsets</th>
<th>Handsets</th>
<th>Handsets</th>
<th>Handsets</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>iPhone iOS 6.1</strong></td>
<td><strong>Android 4.2 Jelly Bean</strong></td>
<td><strong>Blackberry OS 10</strong></td>
<td><strong>Windows Phone 8</strong></td>
</tr>
</tbody>
</table>

### Design
- **iPhone iOS 6.1**: Top hardware build quality, iPhones and iPads have high resale value.
- **Android 4.2 Jelly Bean**: Only 1 device to choose from per 12-18 months, smaller screen size is starting to feel limiting.
- **Blackberry OS 10**: Blackberry controls the hardware and software, which allows them to ensure that they work well together.
- **Windows Phone 8**: Great looking, colorful handsets, good specs and build quality, with Nokia leading the way.

### Affordability
- **iPhone iOS 6.1**: Expensive unless you go for an older model. Expensive unless you go for an old model. But older models don't include features like Siri.
- **Android 4.2 Jelly Bean**: Andromax, BQ, LG, MOTOROLA, Nokia, Samsung, Sony Ericsson.
- **Blackberry OS 10**: Just launched, only the Blackberry Z10 currently available, though 2 more should be arriving soon.
- **Windows Phone 8**: Just launched, small selection of phones, Handsets with large screens available.

### Variety
- **iPhone iOS 6.1**: Large variety, many models and colors, but no suitable BlackBerry.
- **Android 4.2 Jelly Bean**: Lots of phones to choose from, ranging from average to excellent build quality, offering different features such as physical keyboards.
- **Blackberry OS 10**: Handsets with large screens available.
- **Windows Phone 8**: Microsoft's strict hardware requirements, mean there will be less handset variety than Android.

### Performance
- **iPhone iOS 6.1**: Good performance and stability, performance issues for older models when running the new OS versions.
- **Android 4.2 Jelly Bean**: Generally good performance, some devices allow 2 apps to run on a split screen, detailed reports let you monitor performance closely.
- **Blackberry OS 10**: Performance and some cheaper phones, true real-time multi-tasking lets you see the status of multiple running apps at once, QNX technology should provide a more stable and secure foundation to build on compared to competitors.
- **Windows Phone 8**: Good performance - Microsoft has strict hardware requirements.
**Battery Life**

- Battery is not user-replaceable
- Many phones have poor battery life unless you spend time tweaking the settings
- Blackberry no longer has the excellent battery life that it had in the past
- The Blackberry Z10 launch handset has battery issues

**Storage**

- No expandable memory
- Expandable memory available on most handsets
- Expandable memory, good memory management
- Expandable memory available on most handsets

Flagship Nokia 920 handset comes with wireless charging
## Connectivity

<table>
<thead>
<tr>
<th></th>
<th>iPhone iOS 6.1</th>
<th>Android 4.2 Jelly Bean</th>
<th>Blackberry OS 10</th>
<th>Windows Phone 8</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MAPS</strong></td>
<td>![Maps Icon]</td>
<td>![Maps Icon]</td>
<td>![Maps Icon]</td>
<td>![Maps Icon]</td>
</tr>
<tr>
<td><strong>Syncing &amp; Backup</strong></td>
<td>![Sync &amp; Backup Icon]</td>
<td>![Sync &amp; Backup Icon]</td>
<td>![Sync &amp; Backup Icon]</td>
<td>![Sync &amp; Backup Icon]</td>
</tr>
</tbody>
</table>

### iPhone iOS 6.1
- **Maps**: The new Google Maps app is excellent - with better usability than the Android version.
- **Syncing & Backup**: iCloud comes with 5GB free and auto sync photos, books, music, docs, calendar, contacts, and email. Does wireless backups automatically.

### Android 4.2 Jelly Bean
- **Maps**: Google Maps is speedy and has deep integration with other Google services.
- **Syncing & Backup**: Wireless automatic syncing via 3rd party apps. Excellent syncing with Google services Google sync, drive.

### Blackberry OS 10
- **Maps**: Google Maps uses outdated and inconsistent design, not as good as the iOS version.
- **Syncing & Backup**: Wireless syncing via Blackberry Link. Blackberry Protect auto backs up contacts, texts, calendar and bookmarks.

### Windows Phone 8
- **Maps**: Maps can be downloaded for offline use. Nokia Maps has fantastic map data from Navteq, a leading Satnav mapping company.
- **Syncing & Backup**: Syncing via drag and drop, can sync songs and playlists via Windows Media Player or iTunes. Automatic cloud backup, and 7GB free storage with SkyDrive.
### Updating

**Pros:**
- Standardized over-the-air updates
- New OS versions tend to be remain compatible with older handsets

**Cons:**
- Fragmentation leads to long delays and disorganized updates. It's best not to expect an OS upgrade when you buy an Android phone, unless it's a Google Nexus

### Wallet & NFC

**Pros:**
- Passbook stores personal info, membership cards, coupons, tickets etc
- No NFC technology for exchanging data or making payments by touching devices
- Google Wallet lets you store credit card and payment info
- Android Beam allows simple sharing of content between Android phones

**Cons:**
- Blackberry has partnered with Visa to make card payments via NFC

Microsoft has abandoned Windows Mobile and Windows Phone 7 in recent years, which is worrying if you're looking for long term support

**Pros:**
- Wallet stores financial data, tickets, allows wireless payments over NFC, and supports Paypal and in-app purchases
<table>
<thead>
<tr>
<th>Device</th>
<th>Email &amp; Messaging</th>
<th>Email &amp; Messaging</th>
<th>Email &amp; Messaging</th>
<th>Email &amp; Messaging</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>iPhone iOS 6.1</strong></td>
<td>+ Very good email implementation</td>
<td>- iMessage sends free texts, pictures, and video between iDevices and supports group chat</td>
<td>+ Excellent keyboard with gesture typing for faster single-handed typing. Also replaceable, so you have a lot of flexibility</td>
<td>- Hub unified inbox brings together all communication from different sources - even 3rd party apps like WhatsApp</td>
</tr>
<tr>
<td><strong>Android 4.2 Jelly Bean</strong></td>
<td>+ Very good email implementation</td>
<td>Full Gmail integration</td>
<td>- Physical keyboards are no longer standard, which may be a big adjustment for seasoned Blackberry users</td>
<td>- Voice input for texting and messaging</td>
</tr>
<tr>
<td><strong>Blackberry OS 10</strong></td>
<td>+ Innovative keyboard. Select predicted words with a swipe, swipe to delete. Supports 3 languages simultaneously</td>
<td>- BB Messenger service is still excellent, and now has voice/video chat, screen sharing, and can be integrated into other apps</td>
<td>- No push email, contacts or calendar except for Exchange accounts</td>
<td>- Multiple conversations across Twitter, Facebook, Windows Live Messenger, texts, and emails are merged smoothly</td>
</tr>
<tr>
<td><strong>Windows Phone 8</strong></td>
<td>- Can't flag IMAP emails</td>
<td>- Poor GMail integration</td>
<td>- Contacts can be grouped into 'Rooms', with separate calendars and messages</td>
<td>- Landscape keyboard leaves wasted space</td>
</tr>
</tbody>
</table>

**Email**

- **iMessage**: Sends free texts, pictures, and video between iDevices and supports group chat.
- **Gmail Interface**: Wide-spread and cross-platform.
- **Exchange Accounts**: Supports Voice input.
<table>
<thead>
<tr>
<th>CONTACTS &amp; SOCIAL MEDIA</th>
<th>CONTACTS &amp; SOCIAL MEDIA</th>
<th>CONTACTS &amp; SOCIAL MEDIA</th>
<th>CONTACTS &amp; SOCIAL MEDIA</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Contacts &amp; Social Media</strong></td>
<td><strong>Contacts &amp; Social Media</strong></td>
<td><strong>Contacts &amp; Social Media</strong></td>
<td><strong>Contacts &amp; Social Media</strong></td>
</tr>
<tr>
<td>Sync contacts and calendars, and easily post to Facebook and Twitter</td>
<td>Social media apps will integrate with the OS when installed</td>
<td>Contact manager combines all updates from social media</td>
<td>Rooms group messaging feature only works with Windows Phones, which makes it rather unusable in practice</td>
</tr>
<tr>
<td>Facebook is closely integrated, allowing easy sharing of content</td>
<td>No integration by default</td>
<td>Hub pulls in social media</td>
<td>Pulls in relevant info for a contact, such as company news</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>VOIP</th>
<th>VOIP</th>
<th>VOIP</th>
<th>VOIP</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>VoIP</strong></td>
<td><strong>VoIP</strong></td>
<td><strong>VoIP</strong></td>
<td><strong>VoIP</strong></td>
</tr>
<tr>
<td>Many apps available including Skype</td>
<td>No integrated voice-only VoIP</td>
<td>Google Talk has voice chat</td>
<td>Skype is integrated, and other VoIP apps can do the same</td>
</tr>
<tr>
<td>3rd party apps can be integrated into the dialer</td>
<td></td>
<td>Blackberry Messenger has voice chat</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>VIDEO CALLS</th>
<th>VIDEO CALLS</th>
<th>VIDEO CALLS</th>
<th>VIDEO CALLS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Video Calls</strong></td>
<td><strong>Video Calls</strong></td>
<td><strong>Video Calls</strong></td>
<td><strong>Video Calls</strong></td>
</tr>
<tr>
<td>Facetime video calling to Apple devices</td>
<td>Google Talk allows multi platform video chat via Gmail</td>
<td>Blackberry Messenger has video chat and screen sharing</td>
<td>Skype is fully integrated and allows cross platform video chat</td>
</tr>
<tr>
<td>Plenty of video calling apps like Skype</td>
<td>Google Hangouts allows group video chat</td>
<td>Plenty of video calling apps like Skype</td>
<td></td>
</tr>
</tbody>
</table>
## Productivity

<table>
<thead>
<tr>
<th>Platform</th>
<th>Notifications</th>
<th>Documents</th>
</tr>
</thead>
</table>
| iPhone iOS 6.1    | + Slick, easy to use notifications  
- Act directly on notifications, e.g., snooze an alarm | + iWork is a paid productivity suite that works seamlessly with the desktop versions  
- Google Drive allows seamless editing of docs and spreadsheets with automatic syncing |
| Android 4.2 Jelly Bean | + Slick, easy to use notifications  
- No visual preview when you receive a message, email, etc - only LED or audio | + Docs to Go provides flexible editing of documents, PDFs, spreadsheets and presentations |
| Blackberry OS 10  | + Very customizable notification system in the Hub, which you can glance at from anywhere using a gesture  
- When the screen is off, you can still see notifications via the LED light | -  
| Windows Phone 8   | + Apps that have been placed as Live Tiles can show notifications  
- No central hub for notifications | -  

*Note: The table above compares the productivity features of different mobile operating systems.*
### Notes
- There is a good selection of excellent note apps in the App Store.
- Built-in Notes app is very basic.

### Calendar
- Full featured calendar, intuitive to use, integrates with Facebook events.
- Google Calendar is excellent, and is integrated into Android.

### File Management
- Can't use phone as a USB drive.
- Can't manage files directly.
- No built-in Bluetooth file transfer.

### OneNote
- OneNote is fast, syncs automatically to SkyDrive, and handles notes, voice, and photos.
- 'Remember' app can store text, images, video, audio, and voice notes, integrates with Evernote and Outlook.
- Can categorize notes.
- Add content to Remember from anywhere in the OS.

### Calendar
- Full featured calendar that also syncs events from Facebook and LinkedIn.
- Conference call info from the calendar pops up automatically.

### File Management
- Manage files on the phone, like a USB drive.
- Dropbox and Box.net are integrated into the file management system.
- Zip files easily.
<table>
<thead>
<tr>
<th>Profiles</th>
<th>Profiles</th>
<th>Profiles</th>
<th>Profiles</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>Multiple user profiles available, but only on tablets</td>
<td>'Balance' feature lets you have different work and personal profiles, with separate logins, apps, contacts, and themes. Companies can limit and control the Work section, and remotely wipe it</td>
<td>Kids Corner puts your phone in a safe mode so that your kids can play with it without messing everything up</td>
</tr>
</tbody>
</table>

### Other Pros & Cons

<table>
<thead>
<tr>
<th>iPhone iOS 6.1</th>
<th>Android 4.2 Jelly Bean</th>
<th>Blackberry OS 10</th>
<th>Windows Phone 8</th>
</tr>
</thead>
<tbody>
<tr>
<td>+ Huge ecosystem of accessories</td>
<td>+ Several security options including Face Unlock which lets you unlock the phone by looking into the camera</td>
<td>+ Excellent security and encryption</td>
<td>+ Data is encrypted</td>
</tr>
<tr>
<td>+ Slick magazine integration with Newsstand</td>
<td>+ Live animated wallpapers look great</td>
<td>+ Photos hub integrates seamlessly into businesses</td>
<td>+ Hubs provide areas for related features e.g. Photos hub combines your photos as well as photos from social media, and features from photo apps</td>
</tr>
<tr>
<td>- Reminder feature has to-do lists and alerts based on time or location</td>
<td>- Flexibile screen saver options including slideshows and news</td>
<td>- No default feature for handling lost handsets</td>
<td>- Text in photos can be translated</td>
</tr>
<tr>
<td>- Good tech support</td>
<td>- Free marketplace can lead to security issues</td>
<td>- Blackberry Enterprise Services integrates seamlessly into businesses</td>
<td>- Windows Phone 8 being closely integrated to Windows 8 on desktops and tablets, it now has a better chance of picking up momentum</td>
</tr>
</tbody>
</table>

Table 1 Mobile Operating System Comparison
3.0 Mobile Role-based Methodology

The role-based methodology by which a device’s management and data protection are dictated by the role of its user or owner is a trend taking place in many organizations that are thinking of new ways to profile the risk of mobile devices and their users.

Mobile device management tools have centered, to date, on device remediation. In many cases, the ability to lock or wipe a lost device, while important, does not do much to protect the data on the device or restrict the way in which the device can be used in terms of capture, storage, and transmission of information.

Roles such as general knowledge worker, contractors, occasional users, and, to a certain extent, managers are often exempt from the toughest controls which require complex device authentication and encryption. That said, there are managerial roles that require ready access to highly sensitive information such as compensation/salary, details which, when stored on the mobile device of a manager, requires a more strict set of controls. In the case of the contractor or occasional user, device risk profile may be sensitive due to the sharing of devices among multiple, occasional users or the introduction to a personal or other organization’s owned device in the case of a contractor.

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Executive</td>
<td>Due to the high visibility of this user, they are susceptible to targeted attacks and planned device compromise. Of highest value may be email and contact data stored on the device for the launch of further spear-phishing attacks and blackmail efforts.</td>
</tr>
<tr>
<td>Manager</td>
<td>Handling employee personnel data and substantial amounts of product Intellectual Property, managers should be viewed in a similar light to compliance-centric workers.</td>
</tr>
<tr>
<td>Compliance-subject Worker</td>
<td>Working in operations areas such as HR and Finance, these users are regularly in possession of data subject to security controls dictated and enforced by various compliance requirements.</td>
</tr>
<tr>
<td>General Knowledge Worker</td>
<td>Due to the nature of their work, general knowledge workers like to have access to basic PIM functionality on their devices.</td>
</tr>
<tr>
<td>Field Worker</td>
<td>Similar to general knowledge workers, field employees may store data on devices when they are out of cellular network range. These users may require additional security controls as a result.</td>
</tr>
<tr>
<td>Contractor/Occasional User</td>
<td>Contractors and other trusted non-employees have access to company data but are not subject to the same controls and policies due to their third-party status. While requiring data to perform their jobs, these users present a management challenge.</td>
</tr>
</tbody>
</table>

Table 2 Mobile Roles Definition
It is also possible for a user to be a member of multiple groups. For example, many key executives also function in a manager role and many managers or even general knowledge workers, because of their industry may be compliance-subject, in the cases of multiple group membership, an employee’s device security posture should default to the most stringent level of controls.

The table below is intended to serve as a mechanism towards, and not a substitute for policy generation. Detailed profiles of the various user groups inside of any organization will likely resemble many of the groups outlined here but also differ in many ways and require more granular, less binary policy decisions. The granularity in decisions around device policy should also be driven by any relevant compliance standards that are likely to be far more prescriptive (with associated penalties for lack of compliance to the letter of the specification) in their demands.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Executive</td>
<td>■</td>
<td>■</td>
<td>○</td>
<td>●</td>
<td>■</td>
<td>■</td>
<td>■</td>
<td>■</td>
</tr>
<tr>
<td>Manager</td>
<td>■</td>
<td>★</td>
<td>■</td>
<td>●</td>
<td>■</td>
<td>○</td>
<td>■</td>
<td>■</td>
</tr>
<tr>
<td>Compliance-subject Worker</td>
<td>■</td>
<td>★</td>
<td>■</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>■</td>
<td>■</td>
</tr>
<tr>
<td>General Knowledge Worker</td>
<td>●</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>■</td>
<td>■</td>
</tr>
<tr>
<td>Field Worker</td>
<td>■</td>
<td>○</td>
<td>●</td>
<td>○</td>
<td>■</td>
<td>■</td>
<td>■</td>
<td>■</td>
</tr>
<tr>
<td>Contactor/ Occasional User</td>
<td>●</td>
<td>■</td>
<td>○</td>
<td>●</td>
<td>■</td>
<td>○</td>
<td>○</td>
<td>■</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Policy Coverage</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Required</td>
<td>■</td>
</tr>
<tr>
<td>Nice-to-have</td>
<td>●</td>
</tr>
<tr>
<td>Not Required</td>
<td>○</td>
</tr>
</tbody>
</table>

Table 3 Mobile Roles Matrix
4.0 Mobile Platforms Ratings

The analysis of the mobile security experts reveals that today’s mobile platforms widely differ in terms of security and manageability capabilities. As a group, modern mobile platforms provide substantially better security than traditional desktop operating systems when it comes to built-in security mechanisms, authentication, and data protection; even though they are vulnerable to attacks that don’t affect desktop PCs. Application security, device management, and corporate email support are somehow sufficient although they still have room for improvement. The feature sets that IT managers should give high consideration to include: security certifications, device firewall, and support for virtualization, which are largely still missing.

Figure 1 Ratings by Category
4.1 Apple iOS

Now at its fifth iteration, the leading challenger is Apple iOS. Apple’s proprietary approach has become more enterprise-friendly: the strict control exerted by Apple on the overall ecosystem from hardware to operating system to applications makes this platform more secure and manageable in the consumer mobile segment. However, in contrast to RIM’s fully integrated approach, the back-end components required to secure and manage Apple mobile devices are not provided directly by Apple but by a multitude of third-party vendors usually positioned in the Mobile Device Management segment. When complemented by third-party infrastructure, Apple iOS security and manageability are already good enough to be considered for mobility roles requiring device encryption and policy control.

4.2 Android

Despite its impressive market performance, Android security and manageability are the lowest in the segment. The Google Android operating system is at its fourth commercial iteration and has recently seen some important security additions, such as device encryption support, however good Mobile Device Management APIs and a reliable control of the overall operating system versioning and application ecosystem are still conspicuous by their absence. The system is widely exposed to malware and data loss, and the platform fragmentation resulting from the rich OEM ecosystem has proved quite challenging for enterprise adoption. IT managers should definitely consider adding Android to their set of flexible policies but should probably limit its use to the least sensitive mobile roles.

4.3 Blackberry OS

When it comes to individual platforms, the experts’ analysis clearly points out that some operating systems are more mature than others. BlackBerry OS scores very highly across the board, clearly separated from the group of the three emerging consumer mobile platforms. Corporate-grade security and manageability make this platform the option of choice for the most stringent mobile roles.

4.4 Windows Phone

Although last to enter this segment, Microsoft Windows Phone performs quite well across the board especially considering that version 7.5 has only been out for less than 18 months. The system is too new to show a reasonable track record for enterprise adoption, and
corporate policies should take this reality into consideration when considering Windows Phone devices for mobile roles other than for general knowledge workers.

Figure 2 Ratings by Mobile Platform
5.0 The Security Posture of Major Mobile Operating Systems

5.1 Apple iOS

User experience for Apple includes the quality of the applications that are provided to users in the App Store. Apple has very strict guidelines for the approval process of the applications that third parties develop. This goes beyond user interface guidelines, but also to application performance management and in that, they include security. The iOS application architecture natively provides users much protection in terms of the fact that all applications are “sandboxed” in a common memory environment. The downside of this architecture is that theoretically you are only as strong as your weakest app. Security in iOS also extends to the physical attributes of the iPhone and iPad. There are no options for adding removable storage, which in effect provides another layer of protection for users.

Security within iOS takes on other levels, specifically where no application can be installed or updated without the express consent of the user. Even if a company uses a mobile application management solution to “push” applications to an employee, the user still has to approve the installation request for the application to be on the device. This is because iOS is a user-centric mobile operating system.

One historical complaint of the iOS platform was that it did not have the same levels of security as the BlackBerry operating system. That was a very fair comment given that when iOS first came out, it had zero IT management policies, versus BlackBerry’s 500+ (at that time). Today, iOS provides third-party mobility management Independent Software Vendors (ISVs) for a number of native APIs that provide very competent “device management” capabilities (albeit nowhere near the 700+ that BlackBerry has). Again however, there is a difference in terms of the fact that with the BlackBerry platform, the IT administrator has complete control over the device, whereas in an iOS world, the IT department can configure certain things, but only once the user has provided certain permissions to the IT administrator.

Apple has radically changed the world’s views on mobile security, moving it from a world where all policies were dictated by the IT department (regardless of how that impacted the actual users) to a model where the IT department has to now balance the needs of both the workplace and the workforce.
5.3 Google Android

Android has been designed from scratch, with security in mind. It is a privilege-separated operating system and applications cannot access the network without prior consent. Apps run in their individual sandboxed environment, and permissions are granted by the user on a per-app basis. Unfortunately, the end user often fails to closely inspect the permissions request dialogue in their haste to use the app and, for the average end user, it is unclear when permissions are given and what the application is actually capable of. Once the application is installed, the OS does not recheck with the user and goes on to use the permissions without prompting the user again.

This model, while theoretically more secure than the common sandbox on Apple iOS, has the net effect of putting each user in charge of their own security, rather than the operating system. The latest version of Android 4.x does include full device encryption for data protection and Address Space Layout Randomization (ASLR) for buffer overflow protection; however the fragmentation of the handset market means that Android 2.x is still the most widely deployed and provided on the majority of new handsets. Another side effect of this market fragmentation is that there is no central means of providing operating system updates. Security patches are provided to customers by individual carriers or handset manufacturers.
There is an unacceptable delay in this process, meaning that many consumers remain unprotected from critical vulnerabilities for a prolonged period.

Android is currently the preferred platform by cybercriminals. With clever social engineering, they convince a victim to install a “useful” application. The user willingly gives permission and this causes the device to be compromised. Premium SMS fraud Trojans are a costly reminder of unfriendly apps, but what is worse is the data exfiltration function of some of the digital nightmares, malware can copy SMS, intercept calls, remotely activate the microphone, or conduct other threatening tasks.

Attackers are using Android app stores as distribution mechanisms; they promote their apps through online marketing activities, which include sending out spam messages. This is facilitated through the lack of up-front validation of apps after they are submitted to app stores and before they are made available for download. It is compounded by the third-party app store functionality inherent in the Android app model. This open ecosystem is abused by the bad guys, and this will not stop until app store providers themselves establish strict reputation checking. Advising the user to only download from a trusted source does help to mitigate some of the risk, but this also has a downside.

Users tend to see the official Android Market, now called Google Play, as a trusted source, yet multiple examples of malicious code are regularly found being distributed through this official channel. Effective social engineering often makes it complex to figure out if the publisher is a good one or a bad one. The responsibility is with the app store provider, and we hope to see stricter controls there. Google recognized this, and introduced Google Bouncer on the 2nd of February 2012 to “bounce” malicious apps, but there are still unfriendly apps in their store.
5.4 BlackBerry OS

The BlackBerry 10 OS is distinct from any previous BlackBerry OS in that it provides a way to separate out personal applications from corporate-designated ones by using a capability built directly into the OS called Balance. This causes the phone to be partitioned into two spaces, a workspace 100% controlled by IT, which can delete it without interfering in the personal side and represents a way that businesses can support the BYOD trend by allowing employees their personal space on BlackBerry, too.

Although this BlackBerry Balance dual-partition capability for BYOD is not available for Google Android or Apple iOS devices, BlackBerry management can support these non-BlackBerry devices. It simply involves adding a specialized app to iOS and Android devices to do that. Through use of the server-based BlackBerry Device Service software for BlackBerry 10, businesses can manage Android and iOS devices as well, though not Microsoft Windows Mobile. Management capabilities include features such as lock, track and wipe.

BlackBerry is also working on what's known as a "containerization" type of technology for applications that could also be used for iOS and Android that would allow IT managers to place something similar to a container wrap around an app based on IT-based policy decisions.

BlackBerry 10 is also supporting data at rest and in transit through encryption, with the ability to swap out encryption algorithms.

In addition to new features like Balance, the advent of the BlackBerry 10 OS has set the stage at BlackBerry to evolve the basic security strategy related to present and future smartphones.
and tablets. For example, BlackBerry recently established a partnership with security firm Trend Micro to assist in vetting apps against malware through the cloud-based Trend Micro Mobile Application Reputation Service. In another partnership with Germany-based Secusmart GmbH, BlackBerry is creating a specialized encrypted mobile voice capability for BlackBerry that would be used by the German government.

These kinds of projects are widening the perspective on what BlackBerry might undertake in the future as pertains to the BlackBerry 10 OS as a platform, including potentially coming up with a set of security APIs that third-party vendors could build to, such as the kind of anti-malware hooks which they do not have today. There has historically been very little malware aimed at BlackBerry because of its core design being highly virus-resistant, but it is growing.

![Figure 5 BlackBerry OS Ratings](image)

### 5.4 Microsoft Windows Phone

In many respects, it seems that Microsoft has learned the lessons of the past and created a reasonably robust and secure smartphone operating system with Windows Phone.

The OS uses a security model similar to the Android platform, in that minimum privileges and isolation techniques are used to sandbox processes or, in Windows Phone terminology, to provide chambers that act as individual process spaces. These chambers are created and implemented based on a policy system that, in turn, defines what system features processes operating in a chamber can access.
Features that may reveal a user’s location or provide a source of private information are called capabilities on the Windows Phone. The Least Privilege Chamber has a minimal set of access rights that are granted by default but these rights are dynamic and can be expanded by using capabilities during the application install. These capabilities are granted during the install process for an application and cannot be elevated during runtime. This reduces any likely attack surface area and ensures that an application discloses all of its capabilities to a user. It achieves this by publishing its capabilities on the application details page in the Windows Phone Marketplace, prompting the user during the process of purchasing the application and when the user is about to use the location capability of the application and device for the first time.

Windows Phone does not support the use of removable data storage media, and the SD slot in the device is only for use by the original equipment manufacturer (OEM). If a hardware manufacturer does provide removable media then the phone will lock the media using an built-in 128-bit key that, in turn, will pair the phone with the removable media, preventing its use in another phone or PC.

The Microsoft Marketplace Hub contains applications that have been submitted by developers who have registered with the application development program. Windows Phone and the Xbox games systems are the only platforms from Microsoft that require the pre-approval of applications before users can run them, despite developers trying to create unofficial apps for the platform. These attempts were subsequently thwarted by Microsoft as they persuaded the developers of ChevronWP7 to withdraw their tool. Developers receive a certificate as part of the registration process as all applications are signed by VeriSign. Unsigned applications are unable to run on a Windows Phone. The registration process includes an identity check for each developer registering with the program. During upload of applications to the Marketplace Hub, content, function, and compliance checks are made on each application against Marketplace policies that maybe in place.

Applications can be revoked in cases of serious security issues or in less severe cases updates can be sent out to users. Applications are developed using managed code, which combined with isolation of applications and the use of a least privilege model, supports the Windows Phone security model. The application security model prevents the Windows Phone Internet Explorer from installing applications and bypassing this model.
None of the major anti-malware vendors were reported seeing any significant malware targeting Windows Phone.
6.0 Conclusion

This document is not intended to forecast adoption or market fate of individual platforms, because these are irrelevant to the IT managers who will likely have to consider some level of support for all of them anyway. Instead, the analytical framework and the experts’ ratings are intended to provide a valuable tool for the definition of sound mobile policies. This allows IT managers to embrace consumerization with confidence and to turn it into a competitive advantage for their organizations.
7.0 References

- National Institute of Standards and Technology (NIST): http://www.nist.org
- Techtarget, Where Serious Technology Buyers Decide: http://www.techtarget.com
- TechRepublic – A Resource for IT Professionals: http://www.techrepublic.com
- GetNetWise | You’re one click away: http://www.getnetwise.org
- Symantec: https://www.emea.symantec.com
- Prohackingtricks: http://prohackingtricks.blogspot.com
- TrendMicro: www.trendmicro.com
- MyPhoneDeals: MyPhoneDeals.co.uk
- NetworkWorld: http://www.networkworld.com