Best Practices Guide

Mobile Device Management

February, 2011

eAgency, Inc.
6 Upper Newport Plaza
Newport Beach, CA 92660

Table of Contents

Introduction

In today's environment, businesses need to acknowledge the vast array of corporate and personal mobile devices found within an organization. With the rise in available smartphones options, along with the immense applications that are being developed for these devices and being utilized by employees to be more efficient in their personal and professional lives, it is something that can no longer be ignored. Organizations and their IT departments are now faced with the task of managing these devices while protecting their company data.

Blackbox Mobile is a multi-platform data management and security solution that enables management of risk introduced to the enterprise through the growing use of various advanced mobile devices. Blackbox Mobile off¬ers a secure and reliable hosted solution that allows organizations to ramp quickly with minimal resource commitment.

This document outlines several best practices for Mobile Device Management.

What is Your Mobile Device Policy? Is it Realistic?

To have an effective and realistic policy, it must allow for:

- Multiple device platforms
- Personal and/or hybrid devices

The majority of businesses may already being doing something such as this, but they might be unaware of it. Although many companies have a Blackberry corporate standard, the popularity and rise of smartphones has created a surge of personal mobile devices entering the corporate environment. Chances are employees are bringing in their own personal Android and Windows Mobile devices into their organization and connecting to their corporate Exchange Server.

Ensure Compliance with Password Enforcement, Remote Wipe and Data Archival

To help manage the amount of diverse mobile devices within an organization while adhering with compliance regulations, a company needs to ensure their mobile device management efforts assists in meeting security and compliance requirements.

To align with compliance objectives, organizations should ensure their mobile device management strategy necessitates:

- A strong password requirement
- Requirement that devices automatically lock after 10 minutes of inactivity
- Require devices to automatically wipe after 10 attempted logins or if the device is lost or stolen
- Archival of SMS, call logs and email
- Contextual search to aid in the event of eDiscovery requests
- Instant alert notifications
- Application management
- Back up and restore
- One centralized console to manage multiple platforms

Predictable Cost Containment for Network Usage

Controlling cost is a concern for any organization, but especially for those who conduct international business. The cost of international data roaming charges is one that can quickly add up on business travel. Tracking and monitoring such things to control usage should be a requirement for any organization.

Grant Temporary Access on Demand

There has been a great effort put in by phone vendors to restrict applications to certified and approved applications. However, some business may wish to further control certain types of applications that can be utilized on company approved mobile devices. This control may vary by department or business need, and may need to be on a permanent or temporary basis. Granting access on a temporary basis can be used to fill a business need, without abuse of use.

Web Filtering

Web filtering is a common practice in most organizations, restricting employee access to certain websites while using company devices, such as desktops and laptops. This practice should be extended to company issued and/or approved mobile devices as well. As with application blocking, restrictions for web filtering may vary by department, user or business need.

Backup and Recovery

A backup and recovery strategy is apart of any organization, but this should also extend to the mobile devices within your corporate environment. Any organization which has vital or unique data that passes through its employees mobile devices should ensure that back up and recover be a key initiative in their company mobile device management strategy. Although iPhone and Blackberry devices have partial backup capabilities, there should be a solution which would work across multiple platform devices, since most organizations have multiple device platforms found throughout their company.

Control Email and Data Forwarding for Alternative Enterprise and Personal Accounts

Organizations often deem it important to restrict the copying of data to removable media devices or limit the type of attachments employees can download. Executing a solution such as this is often easier said that done for businesses because a data classification exercise can often be arduous. A more ideal solution might be for an organization to construct different virtual containers for corporate and personal applications and data.