A Practical Approach to Securing and Managing Smart Devices

Sajay Rai, Securely Yours LLC
Philip Chukwuma, Securely Yours LLC
Richard Cozart, Securely Yours LLC

Abstract. We have always said that the strength of an organization’s security program is only as strong as its weakest link. Today in most organizations, this weakest link is the use of smart devices like iPads, iPhones, and Android phones. This article provides a practical approach to managing and securing these smart devices.

Introduction

Most organizations in the past deployed BlackBerry devices for corporate use to access e-mail and provide messaging for their employees. These organizations knew that the security on BlackBerries complied with their security policies. A few years ago, a genius named Steve Jobs changed all that. He announced devices like iPads and iPhones. And of course, Google was not going to be left behind. They made their Android OS available to phone manufacturers for free.

With the advent of these smart devices like iPads, iPhones, and Android phones, organizations are now searching for a secure solution for these devices similar to the one they have for their BlackBerry devices. Several vendors have developed Mobile Device Management (MDM) solutions to assist organizations in managing their smart devices.

Typically, IT organizations are chartered to manage these devices. Before they select an MDM solution, they must engage the key departments within the organization to understand the planned usage of these smart devices and gather requirements. Most IT organizations are surprised when they hear the marketing department say how they are planning to use the smart devices, or better yet hear how the CEO or the CFO is planning to utilize a newly acquired iPad.

We suggest a 10-step approach for organizations to plan, implement and manage an MDM program.

Step 1: During the acceptable use policy development, several questions should be asked and answered by key departments within the organization. These questions help identify the requirements and provide input into the next step of defining the IT architecture. It helps to identify the right solutions, after asking the right questions such as:

- Will all devices be deployed by the organization or will users be allowed to bring their own device?
- Is there a need to separate personal vs. corporate data on devices?
- Is personal use allowed or only corporate use? (Can users play Angry Birds?)
- Will employees agree to abide with corporate security policies (e.g. remote wipe, or recording of their phone calls)?
- Will confidential data be allowed on smart devices and how it will be monitored and controlled?
- What type of smart devices will be allowed? Apple only? Android only?
- How are you going to manage backing up devices?
- Do devices need to connect to a corporate network?
- Which apps would you like to deploy? Corporate apps? Do you need your own marketplace?

Step 2: Once the answers to these questions have been obtained, a draft IT architecture should be designed to support the deployment of an MDM solution. For example: an answer to the question “corporate device vs. personal device” may imply whether an organization can wipe out the entire device if it is lost, or if they need a secure “container” within the device to house the corporate data.

The IT architecture may also address issues like:

- Cloud-based solution vs. internally deployed
- Hosted vs. self-supported
- Scalability and performance issues based on number of devices
- How current IT architecture will support the mobile architecture

Step 3: Once the requirements have been defined and the supporting IT architecture has been designed, security policies to support the mobile strategy should be developed. The security policy may address some or all of these issues:

- Password policy control
- Encryption requirements
- Port control (Wi-Fi, Bluetooth, camera)
- Remote lock/unlock/wipe
- Asset tracking
- Device configuration (VPN, e-mail, Wi-Fi)
- Delivery and control of applications to the device
- Blacklisting/whitelisting
- Audit and monitoring

Step 4: Now you can use the requirements identified during the planning phase to select the right MDM solution. The implementation of the IT architecture is completed and the Proof-of-Concept (POC) or pilot program implementation is completed. Typically a select few devices are managed under the POC or pilot program. Typically the following steps are executed:

- E-mails are identified for the selected device owners
- A self-registry link is sent to the users
- Users enter the registry information and obtain credentials
- Security policies are pushed down to the device
- Device is ready for use
Step 5: Enable the e-mail, contact and calendar features according to the mobile architecture and policies defined during the planning phase. Typically, organizations combine the features available within the ActiveSync/Lotus Notes features with the features in the selected MDM solution. This step brings the same functions that are available on BlackBerries to other smart devices. At a minimum, organizations should enable the e-mail, contact, and calendar features.

Step 6: Within this step, organizations roll out custom mobile applications to the smart devices. There are several decisions you probably made during the planning phase. You probably answered these questions during the planning phase:
- Are you going to have your own marketplace, from where your employees can download applications?
- Are you going to develop applications for Apple, Android, or both?
- Are most of the applications going to be browser-based applications, or will they be native custom mobile applications?
- Will employees download these applications from the Apple App Store and/or Android Market?
- Are you going to develop these applications in-house or will a third party develop these applications for you?

During this step, you will need two major processes:
- Verify that the source code is written based on the guidelines provided by the Open Web Application Security Project. This requires appropriate source code analysis tools and the ability to perform penetration testing of the application.
- Incorporate your corporate systems development lifecycle process in the development of mobile applications.

Step 7: During this step, the smart devices begin to act like a laptop and can remotely connect to the corporate network and access corporate resources like servers, LAN shared drives and other corporate data. The focus during this step is to ensure that the same rugged security features are deployed that are used for your remote laptop connections. You should look into your remote access policy to ensure that it supports the connection of smart devices to the corporate network.

VPN configuration, encryption parameters, and virtualization concepts may come into play as you deploy the right solution for this step.

Step 8: During this step, appropriate measures are taken to ensure that the implemented solution complies with regulatory requirements. If the smart device is going to contain financial data, personal health data, personally identifiable information, or credit card information (and most likely you will if you will store e-mails on your smart device), this data must be secured. In addition, the installed mobile solution must have the ability to produce appropriate reports to satisfy the audit requirements of these regulations.

Step 9: This step is to provide adequate support to monitor and report on the managed devices. Examples of type of reports include:
- Number of devices supported and inventory of the devices
- The current location of each device
- Number of remote wipes performed in a month/quarter/year
- Number of stolen/lost devices

Step 10: This step provides the necessary support to internal/external auditors when they perform their audits. More and more auditors are targeting smart devices as they are beginning to agree that the smart devices are becoming the “weakest link” of their security program.

Other considerations: Some of the other considerations related to smart devices may include:
- Evaluate your current e-Discovery process to see if smart devices need to be included in this process.
- Litigation Hold: during the litigation process, it may become important to include smart devices during litigation hold.
- Export control laws: if your organization deals with certain technologies which have export control requirements, you may want to track smart devices to ensure that the device is not in the countries where export control laws may be violated.

In summary, an MDM software solution plays a key role in helping organizations manage and secure smart devices, but preliminary planning is the key to success when deploying your smart device strategy.
Sajay Rai is the President and CEO of Securely Yours LLC. Securely Yours LLC provides cost-effective innovative solutions in the area of information security, privacy, disaster recovery, business continuity and IT audit. Prior to founding Securely Yours LLC, Sajay was a Partner with Ernst & Young’s Security and Risk Advisory practice for 10 years. Prior to Ernst & Young, he was with IBM for 13 years where, among other responsibilities, was instrumental in starting their information security practice, and led the business continuity consulting practice.

E-mail: sajayrai@securelyyoursllc.com
Phone: 866-531-8620

Philip Chukwuma is the CTO of Securely Your LLC. Prior to joining Securely Yours, Philip was a member the Security and Risk Advisory practice at Ernst & Young for 8 years. Prior to joining Ernst & Young, Philip was a member of the Security and Technology services at KPMG, where he delivered security and technology solutions to clients.

E-mail: philipchukwuma@securelyyoursllc.com
Phone: 214-683-8588

Richard Cozart is a senior security consultant with Securely Yours LLC. He specializes in developing and evaluating secure solutions for mobile and web technologies. Prior to joining Securely Yours, Richard was a software engineer for Accenture and co-founder of the web solutions firm, A-Z computers.

E-mail: richardcozart@securelyyoursllc.com
Phone: 313-460-1885

The Software Maintenance Group at Hill Air Force Base is recruiting civilian positions (U.S. Citizenship Required). Benefits include paid vacation, health care plans, matching retirement fund, tuition assistance and time off for fitness activities. Become part of the best and brightest!

Hill Air Force Base is located close to the Wasatch and Uinta mountains with many recreational opportunities available.

Send resumes to: phil.coumans@hill.af.mil
or call (801) 586-5325
Visit us at: http://www.309SMXG.hill.af.mil

E-mail: phil.coumans@hill.af.mil
Phone: (801) 586-5325
Visit us at: http://www.309SMXG.hill.af.mil