NOTIFY TECHNOLOGY

WHITEPAPER

WHY MobileRMM™ IS NEEDED FOR BYOD

Mitigating risks associated with employee-owned mobile devices.

Notify Technology Corporation

888 Boardman-Canfield Rd, Ste C
Boardman, OH 44512

(234) 228-7100 | sales@notifycorp.com

www.notifycorp.com

Why MobileRMM™ is needed for BYOD

Today, smartphones and tablets have proliferated in the consumer market to the point that nearly every employee comes to work with their own internet-connected device. This means higher potential for an employee introducing security risks to your company or organization. If your company or organization allows employees to bring their own mobile devices to the workplace – you need to consider a BYOD security policy.

Supporting a BYOD practice certainly has some potential benefits, but it also can create potential legal, compliance, and support challenges. BYOD security is often a challenge for SMBs. This stems from the fact that in order to be effective, companies must exert some form of control over smartphones and tablets that are not owned by the company but are employees' personal assets.

Many organizations are not aware of the potential issues with allowing BYOD without any additional mobile device management. In many cases the organization is under the impression that since they are personally owned devices, there is nothing they can do. The goal of this white paper is to provide the awareness to why any organization supporting employee-owned iOS and Android mobile devices should have a BYOD policy that will address the range of security issues these mobile devices can be subject to and what recourse the organization can have to mitigate those issues.

We have compiled a list of 6 challenges that companies and organizations will need to solve when supporting a BYOD program for smart phones and tablets.

1

Creating a Company BYOD Policy

Challenge: A good BYOD policy has two characteristics: Policies are clearly defined, and they are enforced. A BYOD policy should address acceptable use, security controls and the rights of the company to secure and manage the employee-owned device. Companies need to define a BYOD policy where employees are required to have some form of mobile management on their mobile device to protect company data.

Solution: The BYOD policy will explain what is required for an employee to use their personal device to access company email and applications. The company will clarify that the mobile management software will create a separate "work" and "personal" segmentation of their device. The BYOD policy should explain that the security and management oversight will only apply to the company information found in the "work" side of their device. No oversight or privacy breeches of privacy will occur on the "personal" side of their mobile device. Should a mobile device become lost or stolen then the company will initiate a selective wipe that will only delete all the company information/data found in the "work" side while no personal data will be affected.

2

Supporting BYOD Devices

Challenge: Establishing a BYOD policy will require support from the company's IT staff and help desk. As employees want to start using their personal smart phones and tablets to access company information, the IT support staff will need to deal with issues from setting up employee email to installing company approved mobile apps used in their work.

As part of their acceptance of the BYOD policy, an employee will agree to having some form of mobile management to protect the company's data. As a result of enforcement of the BYOD policy, the company may want to restrict information access to an end user from their mobile device unless the employee agrees to enrolling into the company required mobile management platform.

Recommendation: Using MobileRMM will provide a process for implementing a company's BYOD policy. Enrollment of personal devices into the MobileRMM platform is simple and easy. Enrollment will create a separate "work" and "personal" segmentation of their device. All work applications will be pushed down to the devices as well as configuring their company email accounts.

Should an application be hacked in the "personal" side it will not affect applications in the "work" side. Both "work" and "personal" sides are encrypted differently creating an additional barrier for security. Using MobileRMM on iOS devices will restrict managed apps from communicating with non-managed apps.

3

Malware & Viruses on iOS & Android

Challenge: This issue might be slightly controversial, but it needs to be discussed as each company will determine their posture protecting their BYOD mobile devices. We will discuss this topic in more detail in a separate white paper discussing the issue and effectiveness of 3rd party malware/antivirus applications for iOS and Android. Companies may feel more protected by requiring 3rd party Malware/antivirus applications for security and compliance requirements as their BYOD policy.

Recommendation: Use the MobileRMM platform to distribute and manage a malware/antivirus solution specified in your BYOD policy for iOS and Android mobile devices. Companies can also use the compliance functionality of the MobileRMM platform to detect any jail broken iOS or rooted Android mobile devices.

MobileRMM can also be used to enforce a policy to disallow installation of applications from unknown sources typically done by side loading of apps on an Android mobile device. Apple only allows apps from the Apple App store therefore side loading is not possible on an iOS device.

In addition, your BYOD policy should require users to make their best effort to keep their mobile device's OS up to date. Company IT can utilize the Device OS version provided by the MobileRMM platform. Finally, your BYOD policy should require users to highly scrutinize opening links from text message as well as links in emails where the sender is not a known entity.

4

Compliance Requirements

Challenge: An employee using their own personal device could be problematic as they may create a violation of a law, regulation, policy, or contract requirement for their organization. For example, smart phones and tablets used in any form of healthcare related services would fall under mobile HIPAA compliance. A BYOD device without some form of mobile management would be in violation and create a regulatory compliance violation for that organization. Many healthcare organizations are aware of HIPAA requirements but have adopted mobile devices in their day-to-day operations leaving themselves exposed to potential loss of ePHI on a mobile device. In many cases it is a matter of educating the healthcare provider that there is an easy and economical solution for enforcing mobile HIPAA requirements which would establish a Safe Harbor for them should any type of ePHI data lose occur.

Solution: Using MobileRMM a company can enforce various security features that meet the requirements for various compliance standards. For example, meeting mobile HIPAA compliance will require the ability to audit mobile devices accessing patient information, enforce a secure password policy, set inactivity device locking, enforce data encryption, provide remote lock and wipe for lost or stolen devices, and keep device OS updated to the latest release. All these requirements can be configured and enforced by enrolling their mobile devices into an MobileRMM platform.

5

Lost or Stolen Devices

Challenge: If an employee's device is stolen or goes missing, all company information must be secured and protected. If the employee wasn't following company security protocols when using their device, loss or theft could cause a major breach. For instance, the employee might be storing their passwords (both personal and company) in an unsecured notes application, which would make it easy for someone who acquires the device to hack into company proprietary data. Even if the employee followed policy down to the letter, hacking technology has become so sophisticated in recent years that a robust password or fingerprint authentication requirement may not be sufficient to keep them locked out of the device.

Solution: Using MobileRMM any lost or stolen iOS or Android mobile device can remotely be locked and wiped. Depending on the company's BYOD policy, a selective wipe may be issued which only deletes the authorized company resources like email and managed applications running on the "work" side of the mobile device.

6

Employee Termination/Resignation

Challenge: When a staff member leaves an organization, a vulnerability can be created if they continue to have access to company applications from their personal mobile devices. To help ensure an employee can't continue to access a system or app after they leave the company, it is crucial that companies are able to reset passwords and revoke access as soon as the employee is no longer authorized. If a security breach does occur, a company should also have systems in place to enable them to identify the mobile device responsible.

Solution: Using MobileRMM a company will have enrolled and provisioned all employee BYOD devices separating the "work" side from the "personal" side. From the MobileRMM's central admin console, IT will be able to "selectively wipe" an employee's mobile device. This would include the employee's email account and all company managed applications and their associated data from the "work" side on any iOS or Android device regardless of whether the employee was terminated or resigned their position.

About Notify

Notify is a highly experienced ISV focused on delivering a mobile management platform to MSPs and IT services providers. Notify's MobileRMM™ offers a security and management solution for both BYOD and company owned iOS and Android devices. Notify's Partner Program provides all the essential support elements needed by an MSP or IT service providers to offer a mobile managed service to its customers.

Call or email us for more information about Notify's MobileRMM™ and Partner Program.

NOTIFY TECHNOLOGY

888 Boardman-Canfield Rd, Ste C
Boardman, OH 44512
(234) 228-7100 | sales@notifycorp.com
www.notifycorp.com