WHITE PAPER

5 THINGS YOU NEED TO KNOW TO EMPOWER TODAY'S MOBILE WORKFORCE

Introduction

As the lines between work and personal life continue to blur, IT departments are under increasing pressure to support personal-liable mobile devices.

When trying to balance this need where employees use their smartphones or tablets for both work and personal use, organizations need to ensure that security and compliance issues are addressed. But simply locking down a device to protect it limits its usefulness.

Instead, organizations need to take into account the way workers use their mobile devices, the ever-changing rules and regulations related to safeguarding corporate information and data privacy, growing mobile security threatsand how all of this can potentially expose an organization to risk if the proper solutions are not used.

Points to Consider

When developing a strategy and selecting solutions for mobile devices, organizations need to address several factors including:

1. Mobile devices get lost: Americans lost about $30 billion worth of mobile phones in 2011.[1] And unfortunately, most (70 percent according to one industry survey) phones are not password protected.

   This immediately puts all of the data on a phone at risk. Whether a phone is lost or stolen, confidential company information and intellectual property stored in emails or documents is ripe for the taking. Other company data also might be at risk. If a missing mobile device runs corporate applications, such as Enterprise Resource Planning (ERP), Customer Relationship Management (CRM), and Sales Force Automation (SFA), a wealth of information could easily be copied, emailed or stolen.

   Worse, a thief could use a stolen phone's contact list and social media applications to impersonate the owner and launch targeted phishing attacks aimed at the phone owner's co-workers and friends.

2. Data on mobile devices is valuable: Just as hackers have targeted corporate systems in the past, today they are targeting mobile devices with criminal intent. The primary motive for external attacks leading to data breaches is financial gain – companies and devices are hacked to get at credit card or other personal data that could then be used to steal money, secrets or other valuable resources.[2]

3. Employees are increasingly exposing data: Many data breaches today are the work of disgruntled insiders. These employees have access rights to systems and data and abuse these privileges. This is has been a growing problem in many organizations. A study[3] of protected health information (PHI) breaches found that 59 percent of all breaches involved a business associate.

   Without safeguards in place, an employee can easily put a company at risk by simply forwarding an email message with confidential, proprietary, or personally identifiable information or by cutting and pasting data from an mobile business app into an email message or another document.

   In many cases, employees may not have malicious intent, but could still put a company at risk by sharing regulated or protected information from a mobile device.

Points to Consider

4. Mobile devices are now prime targets for malicious code: For years, hackers have shifted their attacks in what can best be described as a "follow the money" strategy. Mobile devices are now the new goldmine. As one industry expert noted: "mobile devices offer new avenues for criminal revenue generation."

   In the first quarter of this year alone, malware on Androids quadrupled.[4] Most malware is installed via rogue apps and games. Increasingly, apps are the ideal vehicles for digital theft because even legitimate programs may request permission to access a user's email or social-networking accounts.[5] In the wrong hands, this information could be used to send phishing emails to coworkers or trick trusting social network friends to click on malicious links.

   If precautions are not taken, this can represent a potential problem when an employee mixes home and work use on a single mobile device.

5. Hackers are finding new ways to infect mobile devices: For years, hackers have rigged rogue and legitimate websites to automatically deliver malicious software to any PC that accesses these sites. In fact, this drive-by-downloading technique has been the leading malware delivery method over the last ten years. And in recent years, hackers have focused on search engines so that their drive-by sites would place high in many search listing. Industry studies have found as many as one in three search results are in fact poisoned.[6]

   Now hackers are shifting this form of attack to mobile devices. Last year, security researchers saw the first websites hacked to deliver malicious software to some mobile devices.[7] While drive-bys have been common for PCs, they now appear to be widening to mobile devices.

What’s Needed?

All of these issues must be addressed when looking to support mobile devices for personal and work activities.

Organizations need to strategize how they can manage devices to prevent harmful security risks. And while some organizations might try to put off making any choices or decisions, time is rapidly running out.

The increased availability of new and more powerful smartphones and tablets, combined with the increased interest in Bring Your Own Device (BYOD) strategies, means personal-liable devices will outnumber corporate-liable devices by 2014, according to IDC.[8]

Certainly there are stopgap approaches that might help in some areas. For example, to protect intellectual property and stay compliant in highly-regulated industries, an organization could simply lock down company-issued mobile devices and prohibit the use of personal-liable devices to access corporate assets. This certainly would help the organization, but leaves the worker with no choice but to use two devices – one for work and one for personal purposes.

Another approach might be to rely on mobile device management (MDM) software to ensure a device maintains the appropriate security settings and can be wiped when lost or stolen. But this approach might have shortcomings if only certain devices are manageable by the software or if it is necessary to block access to some corporate resources.

What is really needed is a broader strategy. Rather than looking at the problem in terms of simple device management, organizations need to be thinking about mobile risk management.

BlackBerry as your Technology Partner

Organizations today need a way gives users a choice in devices and applications yet provide IT with the control to safeguard the devices. This is where BlackBerry® can help.

To address the specific issues of personal and business use on a single device, there is BlackBerry® Balance™ technology for BlackBerry® smartphones and the BlackBerry® PlayBook™ tablets. With BlackBerry Balance, employees can use their BlackBerry smartphones and tablets for business and personal purposes without any compromise. At the same time, BlackBerry Balance lets organizations manage the business data and applications on the devices.

Specifically, BlackBerry Balance technology lets BlackBerry smartphones and tablets access business-critical information, while letting the employee enjoy the consumer-oriented features of the phone.

One key feature of BlackBerry Balance is that it lets organizations make a distinction between work and personal data. The software can identify and isolate each type of data.

For work-related activities, BlackBerry Balance protects email messages and attachments sent to and from a user's work email account, as well as the contacts belonging to the company's email domain.

The work partition of a device can receive approved applications sent through the BlackBerry Mobile Fusion console. And files that are downloaded from the company's network or created by an internal application can be stored on the device's work partition.

When an employee uses the device for personal activities, BlackBerry Balance protects the corporate information in several ways. The software prevents users from cutting, copying and pasting work data into a personal application. Additionally, users cannot back up the work data to another device or media card.

BlackBerry Balance offers additional protection when an employee leaves the company. Organizations can permanently delete work data including email messages and attachments, calendar entries and contacts, applications distributed by way of an organization's BlackBerry Mobile Fusion console.

With this capability, an organization could let employees take their smartphones when they leave the company. This would allow workers to retain all of their personal data (emails, contacts, calendar listings, photos, etc.) without the need to transfer it to another device before leaving the company.

The bottom line is that BlackBerry Balance gives organizations the needed control over its BlackBerry smartphones and tablets. And rather than imposing harsh restrictions on the device's use, BlackBerry Balance allows devices to be used for personal purposes. This can improve employee satisfaction and productivity, since they can use the one device for work and personal purposes.

For more information about BlackBerry Balance, visit:
www.blackberry.com/balance

For More Information

BlackBerry Balance, which is available only on BlackBerry mobile devices, is just the latest entry in the line of BlackBerry mobile management solutions. Organizations can use it to complement BlackBerry Mobile Fusion, a next-generation MDM technology.

BlackBerry Mobile Fusion allows organizations to provision, audit and protect smartphones and tablets through a single Web interface.

BlackBerry Mobile Fusion is a unified MDM platform that lets organizations gain control of its mobile workforce. The software can be used to secure and manage all major mobile devices used in corporations today including BlackBerry smartphones, BlackBerry PlayBook 2.0 tablets and iOS® and Android™-based smartphones and tablets.

For more information about BlackBerry Mobile Fusion visit www.blackberry.com/mobilefusion

www.blackberry.com/balance

1. http://www.usatoday.com/tech/news/story/2012-03-22/lost-phones/53707448/1
2. http://www.eweek.com/c/a/Security/Verizon-Data-Breach-Report-Offers-Scary-Truths-About-Security-887453/
3. http://www.redspin.com/resources/whitepapers-datasheets/request_PHI_Breach_Analysis.php
4. http://www.theinquirer.net/inquirer/news/2189104/android-malware-quadrupled-quarter-trend-micro
5. http://online.wsj.com/article/SB10001424052970203753704577255451640014554.html
6. http://finance.yahoo.com/blogs/the-exchange/poisoned-search-results-more-malware-threat-probably-think-150643365.html
7. http://www.networkworld.com/news/2012/050712-university-network-attacks-258993.html?hpg1=bn
8. http://www.datamation.com/mobile-wireless/7-hot-mobile-trends-for-2012-1.htm