



THE DEFINITIVE GUIDE TO ENTERPRISE MOBILE SECURITY

Strategies and Tactics for Business
and IT Decision-Makers

 **BlackBerry®**

The Definitive Guide to Enterprise Mobile Security.

Published by BlackBerry Ltd. 2200 University Ave. E Waterloo, ON, Canada N2K 0A7

To download PDF or e-book copies of The Definitive Guide to Enterprise Mobile Security, visit www.blackberry.com/BES12

Copyright © 2015 BlackBerry Ltd. All rights reserved.

BlackBerry and the BlackBerry logo are trademarks of BlackBerry, Ltd. or its subsidiaries.

* indicates registration in the United States. All other trademarks are the property of their respective owners.

U.S. Library of Congress Cataloging-in-Publication Data

BlackBerry Ltd. The Definitive Guide to Enterprise Mobile Security.

Edited by Jaikumar Vijayan, Alex Manea and Eric Lai.

p.cm.

ISBN 978-1-63315-080-5

1. Mobile Security. 2. Enterprise Mobility. 3. Information Technology. 4. Mobile Applications.

U.S. Library of Congress Class and Year: TK5103.2 .H84 2015

Library of Congress Control Number: 2015904706

Except as permitted under the United States Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher.

Thanks to:

Project manager: Jill Thater

Copy editors: Kara Yi, Matt Young

Designers: The PD Group – www.thepdgroup.com

Executive Sponsors: Heidi Davidson, David Kleidermacher, Mark Wilson, and Trace Cohen

Read Blogs.BlackBerry.com, and follow us at Twitter (@BlackBerry4Biz), LinkedIn.com/Company/BlackBerry and SlideShare.net/BlackBerry

7 Foreword: Enterprises Lag at Mobile Security, Growing Their Risk Profile Every Day

John S. Chen

CEO and Executive Chairman, BlackBerry Ltd.

Chapter 1

Mobile Evolution

- | | | | |
|----|---|----|--------------------------------------|
| 8 | An Enterprise Mobility Journey | 13 | An Organic Evolution |
| 9 | New Era of Productivity | 14 | Maturing Technologies and Strategies |
| 11 | The Disruptive Power of Mobile Innovation | 16 | Bancolombia Case Study |
| 12 | With Change Come Challenges | | |

Chapter 2

Enterprise Mobility in Regulated Sectors

- | | | | |
|----|---|----|---|
| 20 | High Stakes, High Security | 25 | Cost and Risk |
| 21 | Three Key Questions to Ask About Compliance | 27 | Device, Content and Communication Security |
| 22 | Data Integrity in the Mobile Enterprise | 30 | Australian Audit National Office Case Study |
| 24 | The Anytime, Anywhere Challenge | | |

Chapter 3

Mobile Risk and Loss

- | | | | |
|----|---|----|--|
| 33 | The Mobile Threat Landscape | 40 | Organizations and Mobility Risk |
| 35 | Data Loss and Data Leakage | 43 | Are You Fighting the Right Fight? |
| 36 | Insecure Applications | 44 | Rocky Mountain Human Services Case Study |
| 37 | Other Threats | | |
| 38 | Enormous Implications for Regulated Firms | | |

Chapter 4

Managing Mobile Risk in Regulated Sectors

- | | | | |
|----|---|----|--|
| 46 | As BYOD Limitations Surface, a Look at Other Enterprise Mobility Models | 53 | Corporate-Owned, Business-Only |
| 48 | Exercises in Futility | 54 | Criteria for Choosing Your MDM or EMM Provider |
| 49 | The Search for Options | 56 | Global Insurance Provider Case Study |
| 50 | Choose Your Own Device | | |
| 52 | Corporate-Owned, Personally-Enabled | | |

Chapter 5

Developing an Enterprise Mobility Management (EMM) Strategy

- | | | | |
|----|---|----|------------------------------|
| 58 | Developing a Strategy To Manage Your Mobile Environment | 60 | The Technology Component |
| | | 63 | The Vendor Maze |
| 59 | Only the Means to an End | 64 | Samuel, Son & Co. Case Study |

Chapter 6

Extreme Mobile Device Management

- | | | | |
|----|---|----|--|
| 66 | Risk Mitigation Via Device Level Controls | 70 | Containerization |
| 67 | Password and Authentication Controls | 71 | Over-The-Air Programming and Configuration |
| 68 | Local Encryption | 72 | Additional Controls |
| 69 | Remote Locate and Remote Lock | 74 | Unipresalud Case Study |

Chapter 7

Extreme Mobile Application & Content Management

- 76 Securing Mobile Apps and Content for Use in Regulated Sectors
- 77 Usage Policies
- 78 Enterprise Application Stores
- 78 Application Controls
- 80 Multinational Financial Services Firm Case Study

Chapter 8

Extreme Mobile Policy Enforcement

- 83 How the Right Policies and Data Analytics Can Ensure Proper Compliance
- 84 Get a Handle on Regulated Data
- 86 Enable Location-Based Controls
- 87 Enable a Centralized View
- 88 Data Analytics: Letting Your Data Tell Its Story
- 91 Monitoring for Compliance
- 92 Vepica Case Study

Enterprises Lag at Mobile Security, Growing Their Risk Profile Every Day

By John S. Chen
CEO and Executive Chairman, BlackBerry Ltd.



By now, organizations like yours have probably embraced mobile devices and apps for all of the business and productivity opportunities they bring. However, all of the hard-earned ROI and productivity gains you're dreaming about could disappear the moment a hacker successfully phishes your employees' account information via a crafty text message, or when your customers' financial data is stolen using passwords on an executive's lost device.

These nightmare scenarios are already rather common. According to a BlackBerry-commissioned survey of 800 CIOs and risk and compliance leaders last year, 59 percent admitted that the number of data breaches caused by mobile devices **had increased** in the past year (and keep in mind, those are only the ones they know about). As a result, 68 percent agreed that mobile devices are already the weakest link in their security framework.

Despite the admitted breaches, 61 percent of organizations continue to miscalculate or underestimate the risk caused by mobile, admitted their CIOs or risk and compliance managers. In other words: organizations, even those that are normally very conscientious about security, are doing very little when it comes to mobile security.

Clearly, there is plenty of catching up to do. What's your first move? I would suggest reading this guide book, *The Definitive Guide to Mobile Security*, cover to cover. Produced by BlackBerry security experts, the book provides a strategic overview of ALL the risks that your organization faces today in the mobile-first world.

Aimed at both business and IT decisionmakers, *The Definitive Guide to Mobile Security* also offers actionable tactics for planning and building a bullet-proof security architecture, and how to recover if breaches do occur. The guide is especially relevant to those who operate in high-security, regulated industries such as financial services, healthcare, government, etc.

After reading the Guide, I invite you to continue the conversation with one of the security experts here at BlackBerry, or visit BlackBerry.com to download other informative resources, and/or follow BlackBerry via bizblog.blackberry.com and BlackBerry4Biz to learn more tips on enterprise mobile security.



MOBILE EVOLUTION


An Enterprise Mobility Journey

The growing sophistication of mobile devices, applications and management tools are driving fundamental changes in the enterprise mobility landscape. Mobility has become more than just about enabling employee access to email and a handful of productivity applications. It's about untethering the workspace and delivering applications, data and services seamlessly regardless of device type, network or location. Enterprise mobility is about harnessing smartphones, tablets and other mobile devices to enable real-time connectivity to customers, partners, suppliers and workers.

It's an endeavor that is fraught with challenges, especially for companies in regulated industries like financial services, healthcare and government that have to contend with a slew of regulations pertaining to how data is collected, used, shared and stored. The early experience with Bring Your Own Device (BYOD) strategies has already shown enterprises how messy and complex mobility can get. Corporations deploying mobility applications are being forced to reconsider what "corporate liable" really means when offices are being inundated with a flood of low-cost, powerful consumer devices capable of connecting, downloading and transacting with enterprise data – with or without corporate blessing.

An Amazing Technology Story

For anyone old enough to remember the first clunky Motorola cell phones from 30 years ago, today's smartphones are a marvel of modern engineering. Their sleek, small form factors pack an amazing amount of processing power, storage and performance. Continuing improvements in processor speeds, device connectivity, network speeds and better memory, storage and display capabilities are putting even more power in the hands of employees, sales teams, customers and others.

As PricewaterhouseCoopers (PwC)  notes in its mobile innovations forecast, mobile devices have now reached a level of performance where they can meet – and even exceed – uses previously associated only with desktop and laptop computers. By 2015, PwC expects even average smartphones to pack more than 1.5GB of DRAM and high-end phones to have more than 2.5 gigabytes of DRAM. That's about 65 percent of the memory of standard PCs in 2014.

The story with NAND memory is even more impressive. By 2015, says PwC, falling prices will allow device manufacturers to install – on average – some 50GB of memory on smartphones. Tablets will pack between 128GB and 256GB of flash memory by the end of 2015.

"What will users do with three-times the storage they have now?" PwC wonders briefly, before going on to answer its own question. "Much of it will be used to store more HD video and photos at higher levels of resolution." Or, if you're a music lover, you could store over 30,000 from your iTunes library on a 128GB tablet.

New Era of Productivity

Fascinating as all that might be to smartphone power users, there are plenty of reasons why IT executives, administrators and those who manage corporate risk need to be paying attention as well. Modern smartphones, tablets and other mobile devices are reshaping how people connect to the Internet, interact with each other, transact business, conduct commerce and pay for products and services.

A survey in May 2014 conducted by The (US's) Small Business and Entrepreneurship Council (SBE Council) reported that mobile technologies are saving U.S. small businesses more than \$65 billion a year:

"Among mobile technologies, the 2014 AT&T-SBE Council Small Business Technology Poll found that smartphones are saving business owners the most time

(1.24 billion hours) and money (\$32.3 billion) annually. Tablets (saving 754.2 million hours and \$19.6 billion a year) and mobile apps (saving 599.5 million hours and \$15.6 billion a year) are also providing small businesses with more time."

Employees who have options to work in ways that make the location of work unimportant may respond faster, innovate easier and work together better in teams. By boosting morale, a more flexible approach to the use of IT tools can reduce the cost impact of employee turnover. The investment in mobilizing a workforce is too often focused on the cost of the technology, rather than the value of the benefits it enables. Cost is very measurable whereas productivity gains are often not.



There is clearly a realization that mobile technologies come with productivity benefits as more than 80 percent of Fortune 500 companies have deployed or are testing tablets, and researchers report productivity gains of around 40 percent from such investments.

The productivity gains from enabling a workforce to work remotely are driven by the people, the technology they use, where they go and where they work. The technology needs to enable the business processes around any configuration and change of people, place and/or location. This will depend on how the technology is used and how flexible and future-proof it is.

The strongest demand for a mobile-enabled workplace comes from organizations that interact directly with customers such as financial services, legal, health care, insurance, retail, travel and government. Organizations in these sectors have the opportunity to use mobile technologies and become easier, simpler and better to do business with than their competitors. There is a risk of losing current customers and not attracting new ones unless mobile technologies can be integrated into their way of doing business.

For example, mHealth initiatives have driven huge gains in productivity and cost savings. Rural areas will have a lower coverage of medical personnel and in large countries such as the U.S. and China, there is a need to bridge the gap between urban and rural health care quality. Use of mobile technologies is helping to achieve this with text messages to remind patients of appointments and easier access to patient records. mHealth is being adopted globally, and health care is an area that is ideally suited to productivity gains through the use of mobile technologies. Analysis by PricewaterhouseCoopers (PwC) indicates that annual mHealth revenues are expected to reach \$23 billion globally by 2017.

The Disruptive Power of Mobile Innovation

For enterprises, mobility is no longer just a productivity play, though for many it probably will remain the primary driver. Increasingly, mobile devices are becoming an enabler of new innovation and business opportunities. Smartphones and tablets are enabling transformation that is still only unfolding and will take years to play out. But the signs of disruption are everywhere.

In developing countries, mobile technologies have given businesses and governments a way to bypass older technologies completely and to overcome infrastructure shortcomings that have held back businesses for decades.


Investment management firm Franklin Templeton points to Kenya's mobile money transfer system as one example of the disruptive power of mobile innovation. Launched by a mobile network operator as a way for Kenyans without bank accounts to send and receive money, the service has caught on like wildfire in a few short years and spread to several other countries in Africa, Asia and Europe. Money sent through the network represented a staggering 25 percent of Kenya's GDP by March 2102. In India, notes Franklin Templeton [▶](#), mobile phones and tablets have given retailers a way to directly reach tens of millions of new consumers without the need for major capital



The same features that have endowed **modern smartphones and tablets with such powerful capabilities** have also made them **extraordinarily dangerous from an enterprise standpoint.**

investments on floor space and shopping malls. “Technology and the Internet are linking potential customers to markets at a rate that would have seemed impossible even a decade ago,” the investment firm notes.

Meanwhile, a different kind of disruption is happening in the US and other advanced economies. Smartphones, tablets, and cloud-hosted applications and analytics tools are transforming business processes and blurring the traditional boundaries that used to exist between enterprises, customers, suppliers and business partners. There are really no bright red lines that separate the enterprise perimeter from the outside world. A worker sitting in a Starbucks in Times Square is just as easily able to access data in a data center in Tampa as a worker in Tehran or Timbuktu.

Accenture sums it up nicely in its Technology Vision 2014  report: “Smartphones have turned their owners into digitally augmented versions of themselves – able to catalog and quantify actions throughout the day and access, create, and share an astonishing array of pertinent information that can enable faster, better decisions.” Companies, it says, have the opportunity not only to gather business insights, but to turn those insights into acts in real-time in the real world. “The enormous expansion in intelligent capabilities is rapidly reshaping established operations, paving the way for industry disruption on a massive scale.”

With Change Come Challenges

Any change of this magnitude obviously comes with its own set of challenges. The same features that have endowed modern smartphones and tablets with such powerful capabilities have also made them extraordinarily dangerous from an enterprise standpoint. For companies that must answer to regulators – healthcare, banks and financial services firms, for instance – the enterprise mobility movement presents a particularly big challenge. Risk management practices become of prime importance in a setting where protected customer data, intellectual property and trade secrets can literally walk out the door in a shiny new smartphone or can be accessed from anywhere in the world at any time.

Not all of the threats are of a hostile nature, of course. Enabling true enterprise mobility means being willing to open up the enterprise network to a pretty diverse set of technologies on multiple operating systems and carrier ecosystems. For companies that for decades have operated in a wired environment, the enterprise mobility movement has opened up a slew of new decision points. The proliferation of mobile devices has forced companies to rethink access control practices and introduced new worries around topics including device management, content protection, data leakage and data encryption.

Things may be hard now, but it is only going to get worse as the Internet of Things starts to come online. Analyst firms including IDC and Gartner expect tens of billions of “things” – from everyday items like your fridge, toaster and thermostat to sensors in mission-critical industrial control systems – to become Internet-enabled in the next few years. Not all of them will connect to the enterprise network, but enough of them will to pose fresh challenges for those grappling with mobility issues today. Enterprise IT managers and security administrators who are already worried about smartphones and tablets will have much more to deal with when employees, partners and other stakeholders seek to connect to their networks with smartwatches, digital glasses and other IP-enabled mobile consumer devices.

An Organic Evolution

One factor that has exacerbated enterprise mobility worries is the manner in which mobile devices have infiltrated the workspace. Unlike most IT assets, smartphones and tablets in the enterprise have evolved from the consumer side. The growth of mobile use in many companies has been largely organic in nature and driven by workers bringing in personal smartphones and tablets to the workplace, using them to store corporate data or to access it where they can. At least early on, information technology organizations at many companies were largely left out of the picture and any attempts to curb, or control, the proliferating use of personal mobile devices in the workplace was met with resistance.

Initial BYOD strategies at many companies represented an attempt by IT to implement rudimentary device management controls over the entire device. The policies reflected an attempt by IT to exercise the same control over the mobile environment that they have over the PC, server and network environments. Not surprisingly, the strategy did not go down well with an end-user community that had grown increasingly accustomed to using personal devices at work and that was not willing to cede control of their devices to IT.

Maturing Technologies and Strategies

Over the years, device management tools have helped administrators extend and enforce enterprise security policies on personal devices, for instance requiring strong passwords, encrypting data, restricting Wi-Fi access, enabling remote locking of devices and remote wiping of corporate data. But concerns over personal privacy and the increasingly heterogeneous world of mobile devices is pushing companies to look for more flexible and secure options to device

The proliferation of mobile devices has forced companies to rethink access control practices and introduced new worries around topics like **device management, content protection, data leakage and data encryption.**

management. Rather than focusing simply on locking down devices, the effort is to see if there is a way to harness the full potential of mobile technologies in a way that is also secure and compliant with the regulatory needs of many enterprises.

In recent years, a slew of new enterprise mobility management, content management and application management tools have begun to emerge that promise to help companies along the way to a more flexible

enterprise mobility story. For the many companies that permit the use of personally-owned mobile devices to access corporate data, such EMM, ECM and EAM tools allow a greater degree of data protection and governance in their BYOD strategies.

Even so, some organizations, particularly those in regulated industries, are always going to have a need for corporate-issued mobile devices simply because such devices enable the most robust security. A corporate-

owned asset allows the IT group to implement whatever security and management controls they want on it without having to worry about user privacy or device ownership issues. Instead of trying to carve out a portion of a personally-owned device and enabling it for business use, some organizations have begun deploying corporate-owned devices that also happen to be enabled for personal use. Such dual-use, Corporate Owned Personally Enabled (COPE) devices afford companies the security control they need for meeting compliance obligations while also giving them an opportunity to be responsive to user needs.

As mobile technologies get more deeply entrenched in business operations, companies will find themselves having to constantly evolve and fine-tune their enterprise mobility strategies. There clearly is going to be no one strategy that fits everyone. For each organization, choosing the right strategy means looking at its risk profile, industry and regulatory requirements, the technical solutions it adopts, and ultimately how it plans to harness enterprise mobility.





CASE STUDY **BANCOLOMBIA**

Bancolombia is a group of financial services companies with more than 130 years of industry experience in Colombia. The bank offers a wide range of products and services to a diversified clientele of individual and corporate customers, with a portfolio of more than 7 million customers in the country.



The Challenge


Bancolombia's executives are regularly out of the office in meetings or on extended business trips. But they require uninterrupted access to email and the ability to receive documents, such as internal bank activities or important issues like vacation requests. In the past, they had to rely on desktop email, but often had limited access to computers. Lack of access resulted in delayed answers and approvals from directors and vice presidents.

Communication among the bank's departments was also limited, particularly for sales reps who spent a lot of time on the road, visiting clients.

At the same time, Bancolombia wanted to deliver a unique mobile solution to its corporate customers and other people in the financial and investment sector – an important market for the organization. Many of the people in this sector wanted consistent access to financial reports and the Colombian stock market.

Bancolombia required a solution to improve internal communications among its employees, facilitate financial information, and provide customers with simple mobile banking services for transaction inquiries and transfer of funds. Due to the sensitivity of information being transmitted, the bank also needed to have peace of mind that any communications would be sent and received as securely as possible.





**Concerns over
personal privacy
and the increasingly
heterogeneous world
of mobile devices is
pushing companies to
look for more flexible
and secure options
to device management.**

The Solution

Bancolombia equipped over 2,200 employees from 800 branches with BlackBerry smartphones, including built-in email, calendar and task management functionality.

“Our employees can now use email as if they were sitting in front of their desktop computers,” said David Zuluaga Arango, Infrastructure Analyst Bancolombia.

Employees now communicate and stay in touch with their work groups by using BBM. The organization has added users from other departments, including sales and administrative staff, and has implemented the BlackBerry Enterprise Server to manage their BlackBerry smartphones.

To better serve customers, the Bank launched a mobile banking application for BlackBerry smartphones, developed with TODO1.

In addition to its traditional mobile banking functions, investors can use the app to obtain up-to-the-minute information on the Colombian financial market. The data provided by Bancolombia App is automatically updated on the back-end servers and is available almost immediately for customers, even in the most remote parts of the country, where there might not be a branch. With the application, customers can search for banking services such as bank branches, ATMs, bill pay centers, and Correspondent Banks.

Bancolombia's Benefits

With the BlackBerry solution, executives now have remote access to information and can send approvals by email for vacations and other administrative processes. This has helped them improve decision-making and productivity even when they are out of the office.

The Bancolombia App allows its users to view financial market information on their BlackBerry smartphones, giving them access to financial information such as market index charts and a listing of the shares being traded on the Colombian market.

The app has had great success, with more than 104,000 downloads to date.

ENTERPRISE MOBILITY IN REGULATED SECTORS

High Stakes, High Security

The proliferation of mobile devices in the workplace poses compliance challenges for companies that have to abide by strict rules for mitigating security and privacy risks to personally identifiable and other non-public data. Organizations within government and in regulated industries including financial services, healthcare, and energy have to contend with a slew of mandatory requirements for protecting sensitive data in their control. The definition of protected data, the language used to articulate security requirements and the controls needed for regulatory compliance tend to vary from industry to industry. But at a high level, all regulatory requirements have more or less the same objective: get organizations to put reliable measures in place for preventing accidental, negligent and malicious data access, corruption and loss.

Different Regulations, Same Goals

The Sarbanes-Oxley Act, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the subsequent HITECH Act provisions of 2009, for instance, all require covered entities to implement specific controls for protecting customer and other sensitive data. This includes individually identifiable information such as name, address, birthdate, Social Security number and any information pertaining to the past, present and future mental or physical condition of an individual. With the migration to electronic health records in recent years, issues like two-factor authentication, role-based access controls and remote storage of PHI have become major concerns for healthcare providers, insurance companies and other HIPAA-covered entities.

The Gramm-Leach-Bliley Act (GLBA) of 1999 imposes a similar, more prescriptive set of

security compliance requirements on banks, credit unions and other organizations in the financial services sector. Covered entities have to implement a formal information security strategy, maintain an ongoing risk assessment process and deploy encryption, access control, malware prevention and numerous other controls for protecting the security and confidentiality of customer financial information. Under GLBA, financial institutions have to regularly monitor the adequacy of their risk mitigation measures and be able to identify policy violations and suspicious behavior pertaining to sensitive customer data.

For government agencies, the compliance burden comes in the form of the Federal Information Security Management Act (FISMA). FISMA is designed to ensure a standard and repeatable process for security controls for information systems used by

federal government agencies. It provides a long checklist covering areas including risk assessment, security planning and configuration management, communications controls, identity and authentication, access control, auditing and accountability. Government agencies also have to contend with issues like data classification and tagging to enable proper information sharing between different agencies and departments. FISMA itself has been tweaked considerably since it was passed in 2002, and compliance with its requirements is an important metric of an agency's preparedness to deal with security threats.

Three Key Questions to Ask About Compliance

Three key questions that could inform a decision where compliance is a major consideration include:

1. Do your technology investments enable or hinder regulatory compliance?
2. Are you breaking data protection laws without even knowing it?
3. How will different countries' laws affect your approach to technology selection?

In a regulated environment,
**IT must presume that mobile
devices are inherently
insecure.**





Data Integrity in the Mobile Enterprise

Regulatory requirements, regardless of industry, are aimed at ensuring the confidentiality, integrity and availability of sensitive data during storage, transit and use across multiple enterprise applications and environments. Organizations in protected sectors are required to ensure the right data is available to the right people at the right time. They have to ensure regulated data is protected against inappropriate access or alteration. Many regulations have data retention, archiving and auditing components to them as well. While people often tend to think of these regulations as narrow and very industry-specific, many of these rules can be extracted and applied to almost any industry or data protection challenge.

The growth in mobile device use within regulated industries has required covered entities to extend these same protections to smartphones, tablets and other IP-enabled mobile devices that connect to the enterprise network. But it's a task that's easier said than done. Enterprise mobility presents new operational, management and governance challenges for IT organizations in regulated industries for a variety of reasons.

When moving toward a more open and relaxed security policy such as BYOD, a number of new legal concerns need clarification for each country where mobiles are used and the effect of roaming on local data protection laws. For example:

1. Is inappropriate use still a liability for the company, even if it doesn't affect enterprise data? After all, an employee owning a mobile device will expect to be able to use it however they want.	7. Who is responsible for the support, upgrade, security and replacement of lost devices? For example, what if malware attacks an employee-owned device used within a BYOD policy?
2. If an employee is given a monthly allowance for their mobile costs, is that tantamount to the company assuming liability for the mobile usage and user behavior?	8. How will data be recovered from past and present BYO devices if the organization becomes involved in litigation and the court requires access to employee-owned devices? How can this be done without also offering up to the court private data from the employee? Personal and work-related data are likely to be mixed on a BYO device and the cost associated with sorting through that data (and removing personal information) may be prohibitive.
3. What are the boundaries between work time and personal time and should all device monitoring be disabled outside of office hours?	9. Do third-party software licensing agreements restrict download and access to corporate-owned devices? If third-party software is being used from employee-owned devices, is the organization generating multiple breaches of its agreed license terms?
4. What are the legal implications if an organization accesses an employee's personal data, copies it to a central server and then fails to keep that server secure?	10. Have employees downloaded software "for non-commercial, personal use" on their own devices and then used that software at work, thus exposing the organization to a claim by a third party that the organization has encouraged a breach of license?
5. What is the compliance position on data protection if the organization accidentally wipes an employee-owned mobile without that employee's permission?	
6. If an employee leaves employment, can the organization insist on wiping the device or must it accept that any data stored locally on an employee-owned phone is no longer in its possession?	

While there may be technological approaches to managing liability, it is important that organizations have documented policies that clarify how mobile technologies will be used and how to allocate risk between the organization, the employee and third parties. All employees should agree to such policies before using any mobile connected device, especially a personally-owned one.

The **same capabilities that make mobile devices such a must-have for workers** also make them a **nightmare to secure in a strictly regulated environment**.

The Anytime, Anywhere Challenge

The anytime, anywhere access to enterprise applications and data that is enabled by mobile devices has also made them a lot harder to secure than desktop PCs, laptops and other IT assets that are used from within the enterprise network or connect to it via a Virtual Private Network. As the National Institute of Standards and Technology (NIST) [notes](#), mobile devices have a small form factor, feature local storage and an operating system that is unlike any desktop or laptop operating system. Mobile applications are often available from multiple sources and are acquired and installed with little-to-no IT involvement. Smartphones and tablets can synchronize local data with a remote network, desktop computer or laptop computer. They support Bluetooth, Near Field Communications (NFC) and other personal area network interfaces. Most feature a digital camera and removable media and can even be used as an external storage media for another computing device.

The same capabilities that make mobile devices such a must-have for workers also make them a nightmare to secure in a strictly

regulated environment. Data confidentiality, integrity and availability are a lot harder to enforce on devices that are frequently used in homes, hotels, conference halls and myriad other locations outside the IT organization's control. In 2013, about 3.1 million Americans became victims of smartphone theft, according to Consumer Reports [▶](#). In addition to personal data, many such phones can contain regulated data as well, posing a major security threat for organizations in regulated sectors.

Unlike other IT assets, smartphones and tablets are by definition highly mobile and therefore that much harder to control. As NIST notes, even when a mobile device is used within an organization's facilities, it is often transported from place to place within that facility. Security controls and techniques that work in a PC or notebook environment are inadequate in the enterprise mobility world. The sheer range of device choices, the use of jail-broken devices and the ubiquity of services such as text messaging and social media apps only serve to exacerbate such problems.

Cost and Risk

What is usually missing from Total Cost of Ownership (TCO) models in mobile deployments is attention to detail on the risks associated with change, the knock-on effects and how these impact wider costs.

Not all MDM/EMM technologies are alike. Some allow a great deal of variation in the degree to which their solutions can scale and how easily they can be customized to the evolving needs of an organization, while others do not. The risk premium associated with radical change and the time to realizing successful outcomes after an investment needs to be taken into account, or a TCO calculation is meaningless. Along with the cost of the technology, there is also the cost of creating a project around deploying it and then running it as part of a wider IT strategy. Viewing cost in terms of a simple hardware or software license purchase would be a flawed assumption when budgeting IT spend.

Mobile makes it possible to get more done and do it faster, wherever you are and whatever device you use. For the productivity benefits to be realized, the MDM/EMM needs to act as a secure IT policy management engine, controlling who can access what from their mobiles at any point in time.

Consider an organization that has 10,000 employees and 20,000 mobile network connected devices in use in the U.S. This hypothetical organization may want to roll out another 20,000 secure devices across Europe and Asia over the next two years. To achieve the above common expansion objective, the mobile devices would need to be managed by an MDM/EMM that could:

1. Enable users and devices to be categorized into groups with different IT policies and legally applied, regardless of who owns the device.
2. Support a growing range of mobile devices and OS.
3. Enable rapid security update distribution.
4. Simultaneously support BYOD, CYOD and COPE across different user groups.
5. Easily scale up to potentially hundreds of thousands of connected devices.
6. Reflect the organization's view of what data is to be secured and then secure it.
7. Monitor, detect and apply controls to vulnerabilities such as lost phones, jailbreaking or rooting, unauthorized apps and the practices of contractors and outsourcing partners.
8. Ensure that data captured from devices is both legal and enables advanced analytics in the event of investigations, cost and productivity drives or quantification of return on investment in mobile technologies.



A TCO model may **reflect today's needs, but the underlying technology needs to be future-proof** and very flexible to ensure value for money over time.

A TCO model may reflect today's needs, but the underlying technology needs to be future-proof and very flexible to ensure value for money over time.

In the Legal and Professional Services sector, the way in which people work has significantly changed over the past few years. It used to be commonplace for senior legal practice staff to get the same smartphone with the same IT policies applied as a work-only device.

The preferences of users, and their desire to do more with their device of choice, has led to the IT policy of COBO (Corporate-Owned, Business-Only) being viewed as inappropriate in many law firms. Some firms have since implemented

various forms of BYOD or CYOD and increasingly we see a COPE (Corporate-Owned, Personally-Enabled) approach being adopted to balance security requirements while addressing user preferences.

Regardless of pressure from employees, the security requirements of protecting client data have not changed. The way that people work and the IT policies that need to be applied have changed and so have the risks. A flexible MDM/EMM policy enables secure containerization where work and personal data do not mix so that the business can change its IT policies in a risk-controlled way, without making the underlying MDM/EMM systems obsolete.

Smartwatches are invading enterprises' via employees wrists, reviving the BYOD challenges faced by IT with tablets and smartphones earlier in the decade.

Device, Content and Communication Security

Companies in regulated industries that permit the use of personally-owned or corporate-issued mobile devices at work need to think not just about device security but also about protecting the business content on it. The data that is stored on a CEO's phone, or that of other senior corporate executives, is far more valuable than the \$400 or \$500 that the device itself might be worth. In fact, in the wrong hands, the financial data, sales or marketing information and research or customer data on a top executive's mobile device could literally be worth millions of dollars.

In addition to mobile device management, regulated businesses must also focus on data and application protection as well. Just as there are tools and approaches for device management, there are technologies and processes for managing mobile data that are equally important to implement. The focus should be on protecting data at rest on the mobile device and while in transit between devices. IT organizations also need to pay attention to issues such as data access, usage, storage and removal from devices that are no longer eligible to access the corporate network.

In the wrong hands, the financial data, sales or marketing information and research or customer data on a top executive's mobile device **could literally be worth millions of dollars.**

In addition, businesses in regulated industries need to ensure that employees and others with rights to the enterprise network only have access to properly authorized applications and enterprise data from their mobile devices. They need to make sure that enterprise data is always transmitted in a secure fashion between the mobile device and backend servers. Options such as data encryption for protecting data at rest and transmission become increasingly important.

Certainly, mobile device management controls need to be a part of any enterprise mobility strategy. Strong user authentication measures and device managers that enable remote configuration, remote wipe and remote locking of a device are vital to securing the mobile environment. But they go only so far in enabling the tenets of confidentiality, integrity and data availability. Companies that want to exercise some control over what mobile users can download might have to set up an enterprise application store. There, users can get internally-developed mobile applications as well as approved, commercially available ones. Many will need to have formal processes in place for policy management and for monitoring the integrity of their mobile environment. They will need to build new capabilities for detecting, responding to and mitigating new threats to their mobile environment.

Inherently Insecure

In a regulated environment, IT must presume that mobile devices are inherently insecure. After all, most mobile devices are built for consumers and security is not a priority. Enterprises use third-party software to improve the security of consumer devices with mixed results. NIST and other organizations advocate treating all smartphones and tablet computers as untrusted devices, at least when planning a risk mitigation strategy for enterprise mobility. When developing mobile device security policies and controls, organizations should assume that malicious attackers will eventually acquire all mobile devices and use them to gain access to the enterprise network or steal sensitive data from the devices themselves, says NIST. Organizations should understand the threats and vulnerabilities they face and grasp the consequences they would have to deal with in the aftermath of a successful attack.

A Hybrid World

In such a world, a Bring Your Own Device mobility strategy alone is not enough. Letting workers use personally-owned consumer smartphones to access enterprise data and services is risky at the best of times. It is doubly so in any industry that stipulates strict security and privacy controls for non-public



Hackers aren't always the biggest threat to corporate data. Your own employees can be.

and personally identifiable data. Even with good device and application management controls, enterprise mobility presents risks that often can only be managed by robust, centralized IT intervention and control. Even so, few organizations are likely to be willing to eschew a BYOD model entirely for one where IT has total control over mobile devices and the applications that run on it. Analyst firm Gartner Inc  predicts that by 2017, nearly 50 percent of all employers will actually require employees to bring their own devices to work. Many CIOs and corporate leaders believe that BYOD will drive innovation and help smaller companies go mobile without a huge upfront investment.

Technology managers in regulated companies will therefore have to accommodate a hybrid of operational models for enterprise mobility. While there is always going to be a place for BYOD and personally-owned devices, in many situations, IT managers will find themselves needing to employ multiple enterprise mobility operational models such as COPE and COBO. Companies will need to carefully consider the risk versus reward equation associated with each model and decide which one makes the most sense in their particular situation. For some, only corporate-issued devices will offer the level of standardization and control needed to bring their enterprise mobility environment into compliance with regulatory requirements.



CASE STUDY

AUSTRALIAN NATIONAL AUDIT OFFICE

The Challenge

Due to the sensitive nature of its work, the Australian National Audit Office (ANAO) needed to implement a mobile solution that met its strict security requirements and supported its blended BYOD / COPE policy, while driving enhanced collaboration and productivity through real-time communications amongst its workforce.

The Solution

The ANAO used BlackBerry Enterprise Service (BES) to manage a range of mobile devices, including BlackBerry, Android and iOS.



The Situation

The ANAO is a federal government agency that employs around 350 people.

The ANAO plays an important professional role by contributing both nationally and internationally to the development of auditing standards, professional practices, and the exchange of experiences through participation in various peer and professional organizations.

Because of the nature of its work, the ANAO had strict security requirements and a need for solutions that enable enhanced levels of collaboration and productivity for its staff, whilst supporting its mixed device environment.

“In the past, we used the BlackBerry Enterprise Server 5 (BES5), as this was the only secure mobile device management solution approved by the DSD (Defense Signals Directorate), but it was only rolled out to our senior executives, rather than organization-wide,” said Gary Pettigrove, Chief Information Officer at the ANAO.

The ANAO has now deployed a mobile solution to the majority of its workforce so that auditors, who are often required to be off-site at various government agencies, can work more effectively away from the office. Given that 86 percent of the ANAO’s workforce is mobile, the need for a flexible, secure platform is clear.

Rather than allowing a full BYOD model, the ANAO opted for a combination of BYOD and COPE from a pre-selected range of mobile devices, including BlackBerry,

Apple iPhones, Apple iPads and Android devices. While Pettigrove and his team were impressed with BlackBerry’s device offerings and the enhanced security and productivity they could provide, they also recognized the need to give their staff choice; as most people tend to prefer using their own personal device rather than having to carry a separate handset or tablet just for work.

BES10 Facilitating Greater Access and Efficiencies

According to the ANAO, BES provided a more secure and user-friendly interface than competing MDMs. The success of the implementation has convinced the ANAO to look at broadening the scope of BES to mobilize a number of Line of Business solutions, such as travel expenses and database access.

“Our workforce needs to work fast and flexibly across multiple functions of Parliament, all whilst maintaining the integrity and security of national information. By enabling and protecting our workforce with control over the use of work and personal data, we are driving significant efficiencies among our workforce whilst leveraging the capabilities of BES,” said Pettigrove.

Around 40 ANAO staff opted for the latest BlackBerry smartphones. Following the BES rollout, a survey of ANAO staff revealed that IT user satisfaction increased 15 percent. The respondents particularly liked the ability to use a single device for secure work and personal play.

Future-Proofing and Scalability is All Part of the Service

The ANAO plans to expand the solution beyond its senior executives and roll it out to most of its 350 staff in the coming months. Plans are also afoot to offer staff a virtual desktop and an iPad, all managed by BES.

Pettigrove says he has also been impressed with the ongoing support and advice he and his team have received from BlackBerry.

How it works

- ANAO auditors can now access agency data and apps, securely, flexibly and quickly, whilst out in the field.
- Employees can securely access the network using a range of approved devices, including BlackBerry, Android and iOS products.
- Migration to the latest BES provided staff with a more user-friendly interface and enhanced security, productivity and collaboration.

ANAO's Results

- Significant efficiencies achieved by enabling a cross-platform mobile workforce to acquire greater network access.
- Corporate Owned Personally Enabled (COPE) policy for productivity improvements without compromising the agency's strict information security requirements.
- Auditors work more effectively away from the office, confident they are operating securely.
- ANAO staff user satisfaction levels with IT delivery increased by 15 percent following the BES rollout.



“The ANAO welcomes the consultative approach that BlackBerry is taking with key clients and industries.”

Gary Pettigrove Chief Information Officer, Australian National Audit Office

MOBILE RISK AND LOSS

The Mobile Threat Landscape

New technologies introduce new risks. The advent of mobile technologies has ushered in myriad new security threats for IT organizations and has greatly complicated their task of protecting enterprise data from accidental, negligent and malicious harm.

The two biggest risks are malware and data loss resulting from lost, misplaced or stolen smartphones or tablets containing business data.



The Malware Threat

Smartphones and tablets are vulnerable to physical and network threats just like any other network-connected IT asset. Hackers can break into a phone, take control of it remotely, steal data from it or use it as a conduit to gain broader access to a network. They can send spam and rogue SMS and MMS messages, listen in on calls, intercept text messages and impersonate the owner just like they can with desktop and notebook computers. Data from mobile devices can be intercepted and altered and erased. The same sort of security and data protections that is required for desktop and server assets are required for mobile devices as well.

Security vendors such as Sophos have reported huge increases in the volume of malware directed at mobile devices in recent years. In 2014, Sophos detected over 650,000 individual pieces of Android malware with 2,000 more being churned

out every day. And that's only the tip of the iceberg. As more people start using mobile devices to access and store business data, analysts expect to see a sharp spike in mobile malware.

The Inception and NotCompatible Campaigns

Criminals have begun targeting mobile devices in sophisticated malware campaigns as well. The Inception campaign disclosed by security vendor Blue Coat in December 2014 is one example. Blue Coat discovered the international group of cyber criminals behind the campaign quietly exfiltrating confidential data, trade secrets and intellectual property from companies in the oil, finance and engineering sectors in Russia, Venezuela, Romania and Mozambique. Also targeted were government and military organizations as well as embassies and diplomatic offices in Paraguay, Turkey and Romania.

Sixty-six percent of IT managers acknowledge they found it **difficult to keep up with current and emerging mobile threats**. (BlackBerry research, 2014)

One of the tactics that set the campaign apart from others was the use of malware targeted specifically at mobile devices belonging to select top-level executives at these companies. Blue Coat found the attackers using sophisticated mobile malware tools to gather information from compromised smartphones. In some cases, the hackers were using malware to record incoming and outgoing phone calls to MP4 files that were later uploaded to systems controlled by the hackers. In addition to the malware campaign, Blue Coat also found evidence of the Inception gang using rogue MMS messages to conduct a large-scale, multi-country phishing campaign against targeted individuals. The victims included customers of more than 60 mobile service providers including T-Mobile, Vodafone, O2, Orange and SingTel.

A month earlier, in November 2014, mobile security vendor Lookout Inc. ⚡ warned of another campaign dubbed NotCompatible involving cybercrooks delivering malware on mobile devices with the intention of turning them into spam-spewing bots.

Lookout described the NotCompatible campaign as one of the first instances where previously-hacked websites were being used in a large-scale manner to deliver malware on mobile devices. People who browsed certain websites with their mobile devices inadvertently downloaded NotCompatible malware, turning them into botnets that could be used as spam relays or for launching attacks on other devices and systems.

Such threats hammer home the need for organizations to apply controls on smartphones and tablets for detecting and blocking mobile malware threats.



Data Loss and Data Leakage

Malware threats are not the only issue. Mobile devices also present a huge risk of accidental data loss and exposure. In a study on the Risk of Regulated Data on Mobile Devices ⚡ by the Ponemon Institute, nearly 60 percent of the 798 IT managers surveyed said their companies allowed employees to store regulated data such as Personally-Identifiable Information (PII), financial data and health records, on personally-owned mobile devices. Yet, less than 20 percent had any controls for determining exactly what data employees had on their devices.

Not surprisingly, enterprise executives are more concerned about data loss resulting from lost or stolen smartphones and tablet computers than they are about malicious attackers. In a survey by the Cloud Security Alliance ⚡ of some 200 executives from medium and large firms, respondents ranked data loss from lost, stolen and decommissioned mobile devices as their biggest concern, followed by data-stealing malware. Other concerns included data loss as a result of poorly-written

mobile applications, insecure application marketplaces and hardware, operating system and application vulnerabilities. Gartner predicts that by 2017, the focus of endpoint breaches will shift to smartphones and tablets, away from PCs.

Risky User Behavior

Of course, not all of the mobile risks will come from malicious attackers and loss of mobile devices. Much of it will result from risky user behavior as well.

Gartner expects that 75 percent of all mobile security breaches by 2017 will result from simple application misconfigurations ⚡. As an example, the analyst firm points to the use of personal cloud services via applications installed on smartphones and tablets. Personal cloud applications such as email and file sync and share are not designed to convey or store enterprise data. Mobile device owners who use them for such purposes will expose the enterprise to greater risk of data loss.

Users who jailbreak or root their mobile device to install applications and services of their choice on them are another major threat. Jailbroken and rooted devices are altered at an administrative level and remove many of the application-specific protections and “sandboxing” features provided by

the mobile operating system, the analyst firm notes. Malicious applications can be downloaded on them just as easily as any other applications, putting such devices at higher risk of compromise and data theft, Gartner notes.



Insecure Applications

Poorly-scripted mobile applications pose a serious, and often underestimated security threat. In 2013 Hewlett Packard Security Research reviewed over 2,100 mobile applications used by Forbes 2000 companies and discovered a vast majority of them to be vulnerable to compromise. For instance, 97 percent of tested applications accessed private data including address books and social media pages. More than 85 percent had no measures to protect them from common exploits such as cross-site scripting and insecure data transmission.

Three-quarters of the applications did not use, or had poor, encryption when storing data

such as passwords, session tokens and chat logs, on smartphones and tablets.

Such issues can pose a huge problem for companies. Gartner expects that 254 billion free mobile applications will be downloaded in 2017, while paid downloads will hit 14 billion. Given the staggering numbers, mobile applications are going to present a huge opportunity for attackers to try and break into smartphones, tablets and any other mobile devices employees are using. Smartphones and tablets running vulnerable applications and that connect to corporate PCs or other network assets could provide a great way for attackers to try and gain access to the corporate network and to data sitting on systems behind the firewall.

Other Threats

There are all sorts of other issues that make mobile devices frighteningly risky in the workplace. Almost every single smartphone and tablet can take photos and videos. They can record audio, store a relatively large amount of multimedia files and can access the network via Wi-Fi and cellular networks. In a corporate setting, such functions can be easily abused to steal or compromise business data such as customer records, financial charts, IP and trade secrets. They also pose inadvertent data risks. When connected to a PC, for instance, many smartphones automatically attempt to synchronize data between the two systems, potentially exposing business data in the process. Rogue Wi-Fi access points set up behind the enterprise firewall by users trying to establish surreptitious connections for their mobile device scan also pose a serious security risk.

Attacks Shifting to Mobile

Attacks targeting mobile devices are still relatively rare compared to those targeting the desktop and PC environment. Sophos, for example, says the 650,000 mobile malware samples it counted in 2014 were only a “tiny fraction” of the number of pieces of malware targeting PCs. And yet, no one has any doubt that mobile is the next BIG hacker target.

The mobile environment presents a treasure trove of personal data for the cybercriminal and represents an easy way to get to end users, says Sophos.

Just as there are exploit kits available in the wild for PCs, mobile exploit kits are beginning to emerge as well. The Koler “police” exploit kit discovered by Kaspersky Labs in 2014 is one example. The kit is designed to extract money from victims by scanning their systems for location, device type and other information and then using it to deliver customized ransomware demands. Koler is an example not just of emerging mobile malware kits but also of emerging mobile ransomware. Several security firms predict that mobile ransomware kits that remotely lock up smartphones and tablets till victims pay up will become extremely common over the next few years.

Drive-by downloads targeting mobile devices will become more common, as will mobile botnets, mobile phishing and mobile spam campaigns. Attackers will try and use smartphones and tablets as an entryway to the corporate network in much the same manner that they do with PCs and notebooks. Such devices provide an excellent attack vector because of their persistent connections into the corporate network and because they are generally easier to break into than corporate PCs.

The costs of investing in mobile security are sure to be less than the costs of cleaning up after a breach.

Enormous Implications for Regulated Firms

No company wants to deliberately lose data, but regulated firms are obligated to protect it. Companies that fail to do so, especially if they are shown to be negligent, can still face fines, legal liability and other penalties.

In the rush to understand the technology implications of mobile security risks, companies tend to overlook or downplay their potential economic impact. Modern smartphones and tablets can hold large amounts of data and documents and provide privileged access to enterprise networks and services. Any compromise of a mobile device, either accidental or malicious, can lead to a costly loss of business, customer and financial data. Mobile devices belonging to key business executives can contain data on strategic business plans and negotiations.

Organizations in the healthcare sector have reason to pay particular attention to the economic impact of mobile security breaches. A 2013 benchmark study on Patient Privacy & Data Security by the Ponemon Institute showed that 81 percent of healthcare organizations had a Bring Your Own Device (BYOD) policy in place.

It's almost certain that the vast majority of the mobile devices in use in these organizations contain protected health information. Any loss of such data can cost companies millions of dollars in penalties and fines.

IT departments need to understand the risks and the threats posed by the influx of mobile devices in the workplace and find a way to manage it. It is a task that requires an understanding of not just how mobile attacks work but also their economic impact. The sheer diversity of mobile devices, services and applications can definitely complicate efforts to secure smartphones and tablets. But at the end of the day, the effort and the investments that need to be made in bolstering mobile security is surely going to be a lot less than the cost of remediating a breach. For 2014, the Ponemon Institute pegged the average cost of a data breach at \$3.5 million or about 15 percent higher than the previous year. Companies in regulated industries, especially larger ones, can expect to pay tens of millions more in fines and other costs. For many, the costs of investing in mobile security are sure to be less than the costs of cleaning up after a data breach.



**66 PERCENT SAID THAT IT IS DIFFICULT FOR THEIR ORGANIZATIONS
TO KEEP UP WITH EMERGING MOBILE TRENDS AND SECURITY THREATS.**

**ONE ANALYST
FIRM PREDICTS THAT
75 PERCENT
OF ALL MOBILE
SECURITY BREACHES
BY 2017 WILL RESULT
FROM SIMPLE APPLICATION
MISCONFIGURATIONS.**



mobile devices. In fact, more than two-thirds believed mobile devices to be the weakest link in their enterprise security framework.

Respondents indicated they had been too lax in assessing and guarding against risks such as lost or stolen devices, unapproved apps and cloud services, as well as inadequate separation of work and personal use of devices. Consequences in mishandling these issues could lead to immeasurable reputational damage, significant financial penalties and loss of revenue through the loss of trade secrets, or misappropriated customer data. Indeed, these threats are considered critical enough to prompt

75 percent of those surveyed to acknowledge that their organization's GRC groups should be more involved in developing enterprise mobility strategy.

The findings raise serious concerns about the risk exposure faced by enterprises at a time when mobile challenges are growing. Nearly two-thirds of respondents reported the number of data breaches their organization has experienced via mobile devices has increased in the last year, and 66 percent said that it is difficult for their organizations to keep up with emerging mobile trends and security threats.

Organizations and Mobility Risk

In July and August 2014, BlackBerry commissioned a study covering around 800 individuals in six countries with ultimate Governance, Risk and Compliance (GRC) responsibility. Participants were from organizations with 1,000 or more employees (500-plus in Australia), and represented a cross-section of companies and sectors deploying a variety of mobile operating systems and management protocols.

The research revealed a significant gap between what enterprises understand is putting them at risk with their mobile deployment – and how actively they are taking steps to combat those risks. The gap in understanding how inadequately-managed mobile devices in the workplace can contribute to risk – yet not taking action to mitigate that risk – was evident from the findings. Sixty-six percent of those surveyed acknowledged they found it difficult to keep

up with current and emerging mobile threats, and 70 percent of the same respondents claimed they knew they were more tolerant of risk than they should be with their enterprise mobility. Of note, this figure increased to 76 percent in BYOD environments, while it decreased to 64 percent in COPE environments.

For organizations with GRC demands, this gap between awareness and action is startling – particularly in regulated organizations that claim they are risk-adverse. It could leave IT infrastructure vulnerable to attacks or industry regulation breaches that put organizations – and potentially their directors or senior executives – at financial and reputational risk. The survey found only 35 percent of executives, risk compliance officers and IT managers within large organizations were very confident that their organization's data assets were fully protected from unauthorized access via



There's a huge gap between securing mobile devices and PCs, especially in regulated industries.

Three core themes emerged from the findings:

- **Increasing need for Enterprise Mobility Management (EMM).** Seventy-six percent of study participants said the risk of legal liability and costly lawsuits will increase without concerted efforts to adopt comprehensive enterprise mobility management strategies.
 - Sixty-one percent say their organization miscalculates or underestimates risk by focusing on the device rather than the entire mobility landscape.
 - The head of internal audits at a professional services company interviewed for the study said: “Attitudes are changing with regard to work and where you do it. The danger is that as the behavior changes and we use more mobile technologies, the controls do not keep up.”
- **Reconsideration of BYOD policies.** Fifty-seven percent said that they would consider curtailing policies that allow employees to use their personal mobile devices at work (BYOD) in favor of more secure end-to-end solutions such as Corporate-Owned, Personally-Enabled (COPE).
 - Seventy-seven percent reported that it is increasingly difficult to balance the needs of the business and those of the end user when it comes to mobility.
 - A vice president of technology at a financial services firm said: “As soon as someone is on the news there will be a backlash.”
- **Mobility partners must provide secure, future-ready solutions.** Sixty-nine percent said their methods for choosing mobility vendors need to be updated to reflect the current risk and mobility landscape.
 - Seventy-three percent said they want providers to have security credentials and certifications when determining how best to implement EMM solutions.
 - Fifty-eight percent want their partners to have a clear mobility roadmap and solutions that adapt to changing technologies.

Are You Fighting the Right Fight?

Despite the recent spate of high-profile cyber security breaches reported by large retailers and financial institutions, the majority of survey participants cited more commonplace threats among their top security concerns. Nearly three-quarters of respondents listed data leaks associated with lost or stolen mobile devices as a major security risk. “We treat all devices as warranting very limited trust,” said one IT director, adding that lost phones were his company’s biggest sources of data leakage.

Other end user-related security risks, including the loss of corporate information through the comingling of personal and work

data, made the top of the list. “The biggest threats are when using native experience with no container,” said a vice president of technology.

These concerns overlook the more serious consequences that could result from any reticence to consider how an organization is selecting and deploying mobility, against the context of the organization’s risk profile. This view is supported by the fact most organizations surveyed (79 percent) claim they are well equipped to report on mobility with respect to compliance with regulatory obligations and legislation — but less so when it comes to the potential business impact of less apparent risk scenarios (58 percent).

Download the full report and access self-assessment tools for your enterprise at www.blackberry.com/risktolerance ➤



CASE STUDY ROCKY MOUNTAIN HUMAN SERVICES, DENVER, COLORADO

Rocky Mountain Human Services (RMHS) provides resources, service coordination and training to nearly 10,000 individuals living with intellectual and developmental disabilities and veterans transitioning to civilian life. RMHS employs more than 400 professionals across Colorado and Wyoming, and offers several distinct programs ranging from mental health assessments, to brain injury support, to clinical and behavioral health therapies for children and families.



The Challenge

Based in Denver, Colorado, RMHS staff is spread out across the Rocky Mountains. "Part of my job as the IT Manager at RMHS is to ensure we have the right mobile infrastructure strategy in place," explained Frank Baer, IT Manager at RMHS.

"Many of our employees, such as our Case Managers, are rarely at a desk and rely heavily on having information at their fingertips when meeting with a client. With this in mind, functionality was an important factor when considering mobile technology options. Security was also a top priority as our organization handles very private and sensitive client information."

"We provide our home-care staff with laptops, tablets and smartphones so they can update client information and communicate amongst their teams," said Baer. RMHS needed to upgrade its enterprise mobility management (EMM) solution and smartphones to cost effectively manage all of the devices on its network while keeping in mind HIPAA's stringent compliance and security requirements.

Deploying BlackBerry devices with secure enterprise applications, such as Citrix Receiver or Documents To Go™, has tremendously reshaped how RMHS field workers do their jobs. Through these and other applications, RMHS employees can quickly pull information and review case notes from their devices, which proves to be easier and more secure than carrying around hard copies or laptops. A mobile solution also enables RMHS to achieve a high level of immediacy and ease of productivity. Employees also like having BlackBerry® Hub, which brings together work and personal emails and messages into a single convenient location so they can let their loved ones know what time they'll be home for dinner.

Stronger Security for Patient Privacy

HIPAA established national standards for electronic health care transactions and national identifiers for providers, health insurance plans and employers.

"Under HIPAA, even a patient's name is protected, so accessing patient records through the RMHS issued BlackBerry devices is safer than carrying around hardcopy files, a laptop or accessing them through a Wi-Fi network," noted Baer. "With our employees on the road so frequently and constantly changing locations, it's reassuring to know from a HIPAA compliance perspective that

we can remotely disable an employee's device if it is lost or stolen to ensure private information isn't compromised."

Beyond its encryption technology, BES also offers enhancements to enterprise security and manageability, including new IT policy controls and settings policies, S/MIME enhancements, Secure Voice support, Enterprise authentication enhancements and a new IT command to reset the Secure Work Space password. Having all devices under its control and ownership helps RMHS better serve and protect its clients, and do it within a nonprofit's budget.



MANAGING MOBILE RISK IN REGULATED SECTORS

As BYOD limitations surface, a look at other enterprise mobility models

In developing a sustainable strategy for enterprise mobility, it pays to have an understanding of where we are and how we got here.

Looking at the predominance of personally-owned smartphones and tablets in the workplace these days, it is pretty easy to forget that some of the earliest enterprise mobility projects were actually IT-led and IT-enabled. Well before Apple released its first iPhone in 2007, and HTC the first Android phone in 2008, millions of customers were already taking advantage of enterprise mobility via corporate-issued BlackBerry smartphones. The devices allowed IT departments to provision and deploy mobile productivity and communications applications securely across the enterprise without having to cede control of the environment to end users.

Upending the Status Quo

The BYOD trend upended that management model by essentially putting employees in charge of mobile device deployment in the enterprise. Technology organizations – long used to being at the helm of new hardware, software and service deployments – were pushed into a more reactionary role. Instead of being the ones provisioning the new technology, they became the unwilling caretakers of a constantly-evolving environment populated with consumer devices introduced by employees with little or no prior vetting.

Employers, enamored by the prospect of enabling enterprise mobility without having to spend big stacks of money on mobile devices, actively encouraged BYOD. In 2013, Gartner estimated that by 2017, nearly half of all U.S. companies would actually require their employees to bring personal devices to work. The analyst firm predicted that some 40 percent of all companies would stop issuing corporate-liable endpoint devices entirely as early as 2016.

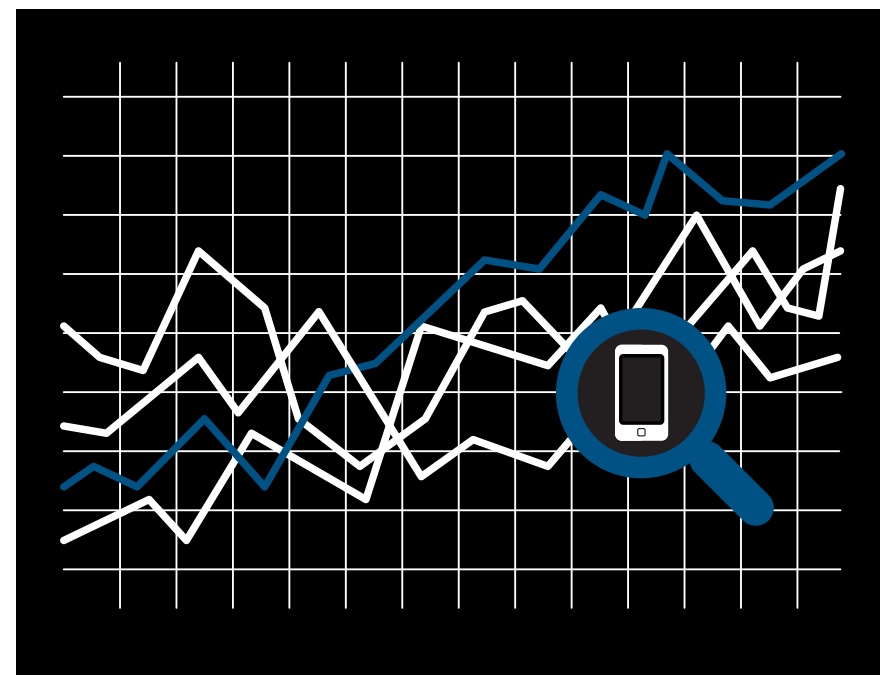
But with an astonishing 90 percent of American workers using their personal devices for work-related purposes like

accessing email and office productivity applications, there are signs that BYOD has gone a little too far. Survey after survey has shown employers and IT organizations admitting to being overwhelmed by the influx of consumer devices. For organizations in regulated industries like healthcare, financial services and government, concerns over data leaks and improper access to enterprise data as the result of malicious, negligent and accidental causes have come to dominate conversations about BYOD in recent times.

A survey of 2,000 IT managers and employees at global firms by Harris Interactive on behalf of AdaptiveMobile found 75 percent saying their BYOD policies were not allowing them to meet a majority of their mobile security requirements. The survey found a bare 11 percent of employees saying they were even aware of corporate mobile use policies. The same Gartner that

predicted most companies would compel a move to personally-owned devices in the next few years, also concluded that there is no way for IT to assume full responsibility for enterprise mobility without some ownership of the devices.

Also, organizations should be careful about approaching BYOD as a cost-saving opportunity. There will be savings on hardware costs (which may be resented by some employees). However, the cost of the physical phone is typically only 20 percent of the total cost of device ownership. These hardware savings will likely be more than offset by the cost of additional security measures, service desk training and workload, changes to financial reporting (“allowances,” for example cannot be capitalized), higher data costs, policy and process changes and new network management tools.



Exercises in Futility

Corporate attempts at exercising control over the environment have worked only partly at best. Employees accustomed to using their personal devices at work have often bogged down such efforts by actively resisting corporate security programs and mobile policies. More than half of the respondents in a Ponemon Institute survey of 618 IT managers and security practitioners cited employee resistance as their biggest obstacle to effective mobile security. About 52 percent said they had to actually scale back on some of their mobile security controls in order to enable greater productivity. Most concerns with enterprise attempts to exercise control over mobile devices have focused on privacy, location tracking, loss of control and restricted device functionality. Even when employers have supplied secure mobile devices for work, the employees have tended to use personal devices anyway simply because they found them easier to use. A staggering 81 percent of 250

respondents in a survey by Azzurri Communications admitted to using their own phones over company-supplied devices, with 21 percent saying they did so daily. A major reason for this is that company-supplied devices are usually out of date and locked down to such an extent that they lose all appeal as a mobile device. Even when a company-supplied device has the same feature set as a personally-owned one, IT organizations can make them completely unappealing by requiring users to input extra-long passwords or by blocking application downloads altogether. Some, like Ovum Research consider BYOD less of a strategy than a behavior that goes on regardless of an enterprise's mobile provisioning and security strategies. Regulatory and compliance requirements, user privacy concerns and the complexity and cost of managing a diverse, heterogeneous array of device have only exacerbated these concerns, Ovum says.

Gartner estimates that by 2017, nearly half of all U.S. companies would actually require their employees to bring personal devices to work.



The Search for Options


As the limitations of the BYOD model have surfaced, companies need to look at models that offer a better alignment between true mobile enablement and control. Several terms have cropped up in recent years that try to capture the essence of what is going on. Examples include CYOD for Choose Your Own Device, COPE for Corporate-Owned, Personally-Enabled and COBO for Corporate-Owned, Business-Only.

	Key Advantage	Key Disadvantages
BYOD	User satisfaction and flexibility (i.e., productivity gains) with the user handling procurement and owning the device	Loss of centralized cost and security control with questions over data protection and auditability
CYOD	User flexibility and satisfaction, but with standardization and control in security and support	Limited ROI on mobility investments as all devices are seen as untrusted with limited access to system and data
COPE	Separation of work from personal usage, data logging and controls, regardless of ownership	None (unless the requirement is for business usage only)
COBO	Simplicity and centralization of procurement and support with full corporate ownership control	Productivity, talent acquisition and flexibility as all employees are obliged to use devices for business only


Each one these models is described in greater detail overleaf. For companies in regulated sectors, the key is not to get hung up on the acronyms and the abbreviations. In developing a strategy, the focus should be on studying the different models and applying them where it makes sense. It is not uncommon for enterprises to have elements of multiple device management options at the same time. The old adages about “no one size fits all” and “no silver bullets” – however trite – are spot on in the mobile environment.

Choose Your Own Device

The struggles that companies have increasingly run into with BYOD programs have spawned interest in CYOD models. With CYOD, a company basically provides a relatively short list of mobile devices and operating systems that they are comfortable about letting employees use at work. Workers select and purchase a device from the list of pre-approved devices and IT then deploys and manages the applications that run on those devices. Employees are free to use the device for both personal and enterprise use within policy limits.

Analyst firm IDC  sees CYOD as a win-win model for enterprises and employees. It predicts companies are increasingly going to adopt CYOD when they realize that BYOD is not the right model for every situation. “Organizations evaluating mobility strategically will look to CYOD as the main adoption model where management and security can be standardized and guaranteed, and business processes can be mobilized,” IDC says.

The goal in giving employees a list of approved devices to choose from, rather than allowing them to bring in arbitrary devices of their choice to work, is to make it easier for IT to exercise control over the mobile environment. With CYOD, the premise is that technology organizations have a lot fewer devices and operating systems to worry about and therefore will have an easier time supporting and keeping track of them. The physical access that IT has to devices in a CYOD model allows companies to provision and apply policies to the devices more effectively.

The perceived advantage for employees is that they get to use personally-owned devices at work with more or less the same freedom available under a BYOD model. The argument goes that employees will be happy so long as enterprises provide a reasonably current, and frequently updated list of devices that are approved for corporate use. As Ovum Research  notes, “a CYOD strategy meets the demand from employees to choose the device they want to use at work, as long as the choice of devices on offer is broad enough.”

There are some caveats associated with a CYOD strategy, say analysts. For regulated enterprises, CYOD offers a more secure approach than BYOD, but for many, that is still not secure enough. Because employees typically still own the mobile devices, IT organizations can never be fully sure how secure the devices remain. As long as IT can only exert partial control over smartphones and tablets in the enterprise, employees could still be able to jailbreak or root their devices, download unapproved applications and access corporate data in a risky manner.

Analysts also believe that CYOD models can only really succeed if workers are given a reasonably current and wide enough selection of mobile devices. Employees that feel their options under a CYOD program are too limited are unlikely to participate in it and will likely resort to using their personal device to access the enterprise network anyway. In an age where mobile devices seemingly become obsolete almost as quickly as they are introduced, the last thing that employees want is to be stuck with a corporate-issue smartphone from the Bronze Age of the mobile revolution.

Even when employers have supplied secure mobile devices for work, the employees have tended to use personal devices anyway simply because they found them easier to use.



Corporate-Owned, Personally-Enabled

A COPE mobile deployment strategy sort of picks up where CYOD leaves off and gives corporate IT a way to gain even tighter control over the mobile environment. The main difference between COPE and CYOD lies in device ownership. With CYOD, it is typically the employee that owns the device. With COPE, the enterprise does.

COPE “provides IT departments with a rich set of levers and knobs to pull and twist in the never-ending and all-important quest to balance end-user satisfaction and business productivity with enterprise security,” says BlackBerry.

Just like BYOD and CYOD, corporate-owned policies offer employees a decent selection of devices and operating systems to choose from for work and play. Since the

devices are corporate-owned, IT has the opportunity to securely carve out separate areas for work and personal use on them, install anti-malware tools and firewalls and set administrative controls to ensure devices remain secure. The model enables employees to use one device for personal and work purposes in much the same way they did with BYOD, but in a much more secure manner.

Or, as BlackBerry describes it, “an archetypical COPE deployment would be one that delivers unfettered productivity and superior user satisfaction, without the nausea-inducing complexity and vulnerabilities associated with loosely-governed BYOD policies.” Both BYOD and COPE extend the use of a consumer device in the work environment, says BlackBerry. But while the effort with BYOD is to try and get a consumer device to work securely in an enterprise setting, with COPE, the goal is to take a securely-configured enterprise device and configure a portion of it for personal use.

The downside with COPE (yes, there always is a downside) is that like CYOD, its success really hinges on the range of choice that employees have with devices and what they can do with them. A COPE strategy that gives users only a limited selection of devices to choose from is unlikely to gain much favor with employees. Similarly, a COPE model is unlikely to go anywhere if users have access to the snazziest smartphones and tablets but can personally do little with those devices because of IT controls.

As the **limitations of the BYOD model have surfaced**, companies need to look at **models that offer a better alignment between true mobile enablement and control**.

Because companies procure and provision mobile devices in a COPE environment, there are few questions over who owns the data or the device used by an employee. Companies that adopt this model may lose the cost benefits of a BYOD model where employees bear much of the upfront capex costs associated with enterprise mobility. However, lower capex doesn’t always mean lower Total Cost of Ownership. BYOD often comes with hidden costs — like the cost associated with managing a plethora of devices and operating systems — that aren’t factored in by many companies.

Corporate-Owned, Business-Only

While CYOD and COPE models can address a lot of the concerns associated with enterprise mobility, there are some situations when only a Corporate-Owned, Business-Only mobile device will do.

The principal characteristic of the COBO device management option, says BlackBerry, is to restrict usage of mobile devices to work-related computing and communications for companies and individuals that require that sort of control. Examples include financial services firms, healthcare organizations and others with onerous regulatory and legal requirements for security.

Company-Owned, Business-Only devices allow for an extraordinary degree of control over the device, how it is used, what data it stores and what functions it can perform. In a COBO environment, IT has total and highly granular control over how the devices are configured and provisioned,

In an age where **mobile devices seemingly become obsolete almost as quickly as they are introduced**, the last thing that employees want is to be **stuck with a corporate-issue smartphone from the Bronze Age of the mobile revolution**.



and what applications run on it. Some support encryption of data at rest and in transit, automated hardware and software integrity checks, application sandboxing and compliance monitoring.

From a security and compliance standpoint, a COBO management option offers extraordinary benefits over any other deployment model. For many organizations, it continues to be an approach that enables the full productivity benefits and operational efficiencies of mobility while also offering the security and reliability assurance needed for regulatory compliance.

Criteria for Choosing Your MDM or EMM Provider

It is important to consider the inherent risks of the MDM/EMM provider as well as the underlying technology of the mobile device. For example, the UK government's National Technical Authority for Information Assurance (CESG) publishes detailed guidance on the risks of working with mobile platforms. Taking a 2014 CESG assessment of a popular MDM/EMM technology, the following types of issues are raised in the End-User Devices Security and Configuration Guidance section:

1. Can the assured data-in-transit protection of the MDM/EMM client be bypassed?	8. Does the MDM/EMM Web-browser and other secured applications override W3C Web Storage APIs (i.e. HTML5 local storage, where websites may store user data)? If such information is not protected, then "malicious or compromised websites may be able to exploit a vulnerability."
2. How reliant is the MDM/EMM on the native platform for providing suitable controls?	
3. Is Secure Boot enabled by the MDM/EMM? Is protection reliant on the native device platform?	9. If secured applications can be unlocked by using a temporary unlock code, how well protected is this security code, and how often is it changed?
4. To what extent can the MDM/EMM supplier's compliance manager provide proof of no malware? Is protection reliant on the native device platform?	
5. Does the MDM/EMM provide sufficient information for usage analysis and investigations?	10. If the MDM/EMM client is contained in a single containerized sandbox, does a vulnerability in one component allow malicious access to all data within the MDM/EMM client? Ideally, there would be isolation between the internal components (e.g. the Web browser and the email client) so that if one component is compromised, it does not then expose all of the rest.
6. Can the MDM/EMM's secured applications choose to communicate directly with Internet services without network traffic being routed via an NOC? I.e. when information is sent outside the security of the MDM/EMM, how protected is it?	
7. While the data sent via an NOC may be encrypted, is the enterprise metadata encrypted as well? If not, an adversary would be able to discover email addresses, registered devices, which applications are running, the enterprise domain names and the specific names of the user accounts used to set policy on the MDM/EMM control panel.	11. Does the MDM/EMM client have its own address book, and if so, does that mean that the client will prevent the device from displaying key information such as the name of the person calling? If not, the approach of synchronizing information with the mobile device's native applications (e.g., phone number, email addresses, notes, personal notes, etc.) places this information outside the safety of the secure sandbox.



This illustrates that there are important questions to be asked about MDM/EMM technology solutions and that not all solutions can be assumed to offer the same degree of usability, security and functionality. The MDM/EMM vendor's approach to security is an important part of the front line in protecting confidential data and ensuring compliance with data protection and other regulations. Since it is often a legal requirement to report breaches, the reputational damage of not having the best possible security in place can have a financial impact as a result of reduced trust and confidence from buyers and suppliers.

While the reputational damage of a breach is hard to quantify, the OnePoll survey of March 2014 indicated that 86 percent of customers would shun brands that have suffered a data breach. When data breaches take place, there is also a potential to lose trust and buyer confidence if appropriate steps are not taken. In a 2014 U.S.-based survey of 797 individuals conducted by Experian and the Ponemon Institute, it was found that "most consumers continue to believe that organizations should be obligated to provide identity theft protection (63 percent of respondents), credit monitoring services (58 percent) and such compensation as cash, products or services (67 percent)."

It is important to consider the **inherent risks both of the MDM/EMM provider** as well as the underlying technology of the mobile device.

CASE STUDY

LARGE FINANCIAL SERVICES PROVIDER, NORTH AMERICA

A global leader in the financial industry, this company has over 100 years of experience, and currently serves nearly 100 million customers across more than 50 countries. To manage it all, they have a workforce that's 70,000 strong.

The Challenge

A long-time BlackBerry customer, this company was in the process of migrating to the latest version of BlackBerry Enterprise Service (BES) – a move that would allow them to manage multiple platforms and device ownership models. So while they were rolling out thousands of new BlackBerry devices, they were also trialing a bring-your-own-device (BYOD) program, allowing employees to use personal iOS phones and tablets for work.

At the same time, the company was looking for a better way to manage its most valuable resource: its workforce. They needed a way to securely track and analyze metrics on how their employees worked. For years, they'd relied on desktop systems and dashboards for HR insights, but they realized that now was the time to give decision-makers mobile access to this information – from recruitment numbers and workforce turnover rates to compensation averages and performance statistics.



The Solution

Deciding where to turn for guidance was easy because of the solid relationship between the company and the BlackBerry team. As Swalé Nuñez, Senior Enterprise Developer on the BlackBerry Enterprise Solutions Team, commented: “We’ve established a great rapport, so when it comes to any kind of application or mobility question, they reach out to me for insight.”

After discussing the requirements, Nuñez proposed a solution during the meeting. Rather than taking on the cost of creating a custom solution, or abandoning the project altogether, the company could apply the required layer of security using the Secure Work Space feature of BES. Secure Work Space would provide the gold-standard BlackBerry security that the company was looking for, even on this iOS version of the app. It would allow them to maintain the app’s integrity and to secure sensitive corporate data – all while avoiding the costly and lengthy process of rewriting code from scratch.

The Benefits

Reaching out to Nuñez and the BlackBerry team saved this company time and effort. Instead of wasting days or weeks with trial and error solutions, they were able to resolve the issue with one phone call. BlackBerry handled the security wrapping process for the customer as part of their service.

Key Benefits

- **Saving time and effort:**

One call to BlackBerry gave them the solution they needed.

- **Saying yes to business goals:**

Instead of putting up barriers, IT delivered on the request while ensuring their security goals were achieved.

- **Freeing up resources:**

Although it’s something the customer could handle in-house, BlackBerry wrapped the app to ensure a timely and secure implementation.

- **Managing it all with ease:**

BES provides a central console through which this company can manage apps, security features, and more in a multi-platform environment.

DEVELOPING AN ENTERPRISE MOBILITY MANAGEMENT (EMM) STRATEGY

What You Need To Do When Developing a Strategy To Manage Your Mobile Environment

A formal Enterprise Mobility Management strategy can help organizations add structure to their efforts to manage the mobile environment. When developing and implementing such a strategy it is vital to have a plan that accommodates BYOD, COPE and COBO models because it is unlikely that a single mobility model will work across the entire enterprise.

Not Just About Security and Control

There often is a tendency to view EMM as being all about security and control. In fact, it really is more about enabling the full productivity and cost benefits of mobile technology in a secure manner. Security is obviously a key underpinning of any EMM strategy, but it is not the only focus. Rather than restricting and controlling mobile access, an EMM strategy really should be more about helping enterprises seamlessly integrate mobile technologies into their business processes so they can derive real

value from it. It needs to be as much about addressing business needs as it is about employee engagement and empowerment.

The 451 Research group predicts that much of the demand for EMM technologies will stem from companies migrating from a reactive to a mobile-first strategy. “EMM is moving from tools that control mobility, to instrumental elements that enable productivity for a growing number of mobile-enabled employees,” says research director Chris Hazelton.

Only the Means to an End

Numerous mobile management products currently help companies implement and enforce security and automate usage policies. They serve a vital role in helping companies gain visibility over their mobile environment and in implementing granular policies for controlling them. Without a formal mobility management strategy though, the tools by themselves do little to enable new and innovative use of mobile technologies. The three most important questions to ask when assessing the effectiveness of your organization’s mobile security are:

1. How much of your company data is on or accessible from the personal phones and tablets of employees, contractors and partners?
2. Has your testing strategy been updated to accommodate developments in new technology as applications enable mobile workflows?
3. Could you defend and limit the impact of a cyber-attack given the changing and dispersed nature of a mobilized workforce?

Furthermore, organizations planning for mobility must:

Define an objective

A good place to start is to define and prioritize organizational goals for enterprise mobility. When mobile devices are properly harnessed they can enable better productivity, improve operational efficiencies, support better decision-making and offer a competitive advantage. It is only by identifying your

organization’s goals that you can begin to develop a plan to support them. Gartner recommends [▶](#) that the IT group collaborate with stakeholders to identify and agree on business objectives for enterprise mobility before architecting any solution for it.

Scope requirements

To understand support requirements, mobility managers need to have a clear idea of the people or groups of people that are or will be using mobile tools. Have a clear understanding of how, why and how often employees are using or will be using these tools at the work place, and determine what applications and services they need in order to support their use of mobile technologies.

Identify gaps

Just because 90 percent of your workforce is already using smartphones and tablets to access email, interact with customers and download data, doesn’t mean your business or your infrastructure is really equipped to handle enterprise mobility. Supporting the always-connected employee means having an infrastructure that is flexible and robust enough to support numerous operating systems, and mobile devices connecting to the enterprise network and data in countless new ways. Are your backend systems equipped to support exponential increases in activity from mobile employees? Can you identify devices that are connected to the network? Do you have the access control and authentication requirements for controlling access to the network and data?



A security strategy needs to be as much about addressing business needs as it is about employee engagement and empowerment.

The Technology Component

Organizations need tools for managing and securing the devices as well as the applications and the data running on them. That means implementing tools for managing mobile devices, mobile applications and the content on mobile devices and networks. Technology vendors use terms such as mobile device management (MDM), mobile application management (MAM) and mobile content management (MCM) to describe some of these capabilities. (See the following chapters for more details on these technologies and the best strategies for using and implementing them.)

Over the years, dozens of vendors have emerged in this space offering a bewildering array of products to help companies achieve varying degrees of control over the mobile environment. This can be a real problem for organizations trying to figure out a technology strategy for enterprise mobility. Many companies fall into the trap of taking bits and

pieces of technology from different vendors and trying to make them fit together, which never seems to work. Many vendors have increasingly begun offering these capabilities as managed services as well. Typical mobility support services include deployment of EMM software, technical and business support for the entire EMM stack and managed Wi-Fi.

The Technology Challenge

Once business objectives have been clearly defined and agreed upon, the IT group needs to develop a plan for implementing those objectives via the strategic use of EMM technologies and services. That can be challenging, given the evolving nature of enterprise mobility and its still-maturing tools.

Product and service vendors sensing a major revenue opportunity have begun to inundate the market with a dizzying array of choices and claims that can be incredibly hard to sift through, not just for the uninitiated but for the technically savvy as well. In an emerging

market, the terms and capabilities used to describe product sets and service are not always consistent. What one vendor might describe as an application management capability, another might lump into the content-management category. While some describe the Choose Your Own Device (CYOD) model as one where the employer pays for the device, others see it as a personally-owned device model where the employer simply has a greater say in the choice of devices that are permitted in the enterprise. The fact that vendors are constantly updating and upgrading their product sets only makes the task of choosing the right EMM technology suite even harder.

This is why it makes sense for those in charge of enterprise mobility projects to focus on the broad objectives rather than on product definitions and categorizations. The goals should always be: increase user productivity, secure corporate assets and keep users happy. Any EMM technology that is chosen

should support a multi-device, multi-operating system environment and allow for varying degrees of security control to be exercised over the environment.

Technology Requirements Scoping

BlackBerry breaks down the task of technology scoping into five specific requirements: physical access security, authentication and end-to-end encryption, remotely manageable hardware controls, personal and workspace segregation and secure applications. The company also advocates the need for enterprises to explore how EMM capabilities can be used to mitigate legal risks that companies in regulated sectors can face from the insecure use of mobile devices in the workplace.

A Mobile Device Management capability is a minimum requirement for your company, regardless of whether you support a completely BYOD model, a company-owned device model or a combination of both. MDM tools allow companies to impose a set of physical controls on the device itself and are therefore a fundamental protection against data loss and theft. MDM products typically support capabilities like password protection, strong authentication, data encryption, over-the-air (OTA) updates and automated policy enforcement. Importantly, MDM products give companies that ability to remotely reset or lock a device or wipe corporate data off it in the event a device is lost or stolen or if the owner of the device leaves the company.


Many companies fall into the trap of **taking bits and pieces of technology from different vendors and trying to make them fit together**, which never seems to work.



Mobile Application Management

Useful as they are, device management tools by themselves do not always offer the flexibility that is needed for true Enterprise Mobility Management capabilities. As companies evolve away from BYOD-only strategies there is also a need for controls over the applications and the content accessed, stored and shared via mobile devices.

Mobile application management tools are critical for ensuring that only approved applications and software run on mobile devices that access the corporate network and data. They offer a way for companies to set up an enterprise store from where users can safely download applications for use, typically a small number of internally-vetted and created apps and approved consumer apps from mainstream public app stores.

Analyst firm ABI Research  sees MAM tools as becoming the enterprise mobility technology of choice for companies over

the next few years. Over the next few years, look for application management tools to not only help companies deploy app stores and application development platforms, but also to help more holistically with mobility and workspace management as well, says ABI.


Mobile Content Management

Another technology category companies will need to evaluate when deploying an EMM strategy is mobile content management. MCM tools address the need for companies to give users a way to securely access, share and collaborate with sensitive enterprise data with their mobile devices. Vendors tout these tools as a safer alternative to the public cloud-based sync and share applications that are being increasingly used by employees to access and share enterprise data. Content management tools offer varying capabilities but typically include some kind of a locker or container for storing sensitive data and functions for accessing that data in a secure manner.

In a market place that is still only emerging, the **terms and capabilities used to describe product sets and service are not always consistent.**

The Vendor Maze

Figuring out which vendors and tools to select for their purposes is another major challenge for enterprises. When sorting through the numerous available technologies and services, organizations should make sure to evaluate product functionality, product maturity, the vendor's service and support capabilities, its enterprise track record and ability to scale.

The 451 Research  group suggests starting by looking at vendors that offer more than just an MDM capability. As your strategy evolves, your vendor must be able to not only keep pace but to actually lead the way on innovation and technology capabilities, it says. Any technology vendor you choose needs to be able to support a deployment strategy that includes BYOD, COPE and even a completely business-owned and business-controlled mobility model. The vendor's ability to scale is a critical consideration to keep in mind, especially considering the still-evolving nature of this product space.

Vendors offering EMM capabilities fall into three broad categories, the analyst firm says. The first category is composed of mobile-only specialists such as BlackBerry. The second category consists of enterprise players that have diversified into the mobile management space in recent years. The third group consists of a new breed of startups focused purely on enterprise mobility. In selecting vendors for EMM, organizations should be careful about mapping their requirements with the vendor's core competencies.

As with making any other selections, companies need to evaluate each technology and vendor on their merits and determine what makes the most sense for their particular compliance and security requirements. For some, a best-of-breed approach might appear to be the most sensible way to go. For others, especially those in heavily regulated sectors, a specialist vendor might be the appropriate choice.





CASE STUDY

SAMUEL, SON & CO.

Founded in 1855, Samuel, Son & Co., Limited, has grown into one of North America's largest family-owned metals processor, distributor and metals manufacturing companies. Samuel operates over 115 strategically located steel service centers and metal manufacturing facilities to offer clients end-to-end solutions in the distribution, transportation, processing and manufacturing of metals and industrial products.

The Challenge

Samuel's employees and clients are dispersed across the world, including in the United States, Canada, Mexico, Australia and China. With a highly mobile workforce, Samuel needed an Enterprise Mobility Management (EMM) solution that would enable seamless mobility within the organization and optimize employee productivity, while allowing IT to control and manage its fleet of devices remotely. "With a vast geographical footprint, we need to be able to reliably communicate with one another and connect to our network securely," explained Bob Carter, Chief Information Officer at Samuel, Son & Co., Limited, "Logistics are vital to our operations, so real-time data and information sharing is key."



The Solution

After a review of other vendors' solutions, Samuel selected BlackBerry smartphones and the BlackBerry Enterprise Service (BES) as their core end-to-end business mobility solution.

"The powerful combination of BlackBerry smartphones and BES offers us an integrated mobile device and server solution that meets our highest security and productivity needs," Carter said.

With this deployment, Samuel continues its long-standing partnership with BlackBerry, by deploying BES and issuing a fleet of BlackBerry devices across the organization.

Samuel also has access to in-person product training support provided by BlackBerry Technical Support Services to effectively and effortlessly bring Samuel's workforce up and running on the new platform.

Benefits in Detail

The BES multi-platform solution allows Samuel to manage BlackBerry, iOS and Android™ devices from a single, highly secure and reliable platform. "When we set out to find a mobility solution, we were confident that BlackBerry would meet our needs.

Mobility is integral to the success of our business, helping to drive the overall level of productivity and fuelling innovation within our organization. We had to be meticulous about our selection process, but we know we made a great choice and the best value proposition with BlackBerry," added Carter.

Samuel also took advantage of BlackBerry Technical Support, which provides distinct levels of support, options that align to the level of expertise, and assistance and resolution time that each business requires. The added assistance has helped the company realize the full potential of its mobile environment, minimize costly downtime and support all users, including those using iOS and Android mobile devices.

"BlackBerry offers best-in-class customer service experience and product training support, which makes deploying BlackBerry a great value proposition overall. The product training support helped in eliminating the learning curve for employees for an easy and effortless transition," said Carter.



EXTREME MOBILE DEVICE MANAGEMENT

Risk Mitigation Via Device Level Controls

There are many ways in which a compromised smartphone can be both the source of and mode for an escalation of attacks on end users and their employers. The key threats include:

1. Unauthorized monitoring and surveillance by gaining access to audio, camera, location, SMS and call logs.
2. Data theft of account details, call logs, address book contact details and International Mobile Equipment Identity (IMEI) numbers.
3. Financial loss through unauthorized premium SMS and phone calls, ransomware, fake anti-virus and compromise of PINs and passwords.
4. Identity theft such as impersonating the user through SMS, emails and social media posts.

While there may be limited publicity around the hacking of smartphones, there is widespread reporting on the increased vulnerabilities that come hand in hand with enhanced smartphone functionality. For example, the tilt sensor on a smartphone can be used to detect and log the keystrokes made on a laptop or PC, or even the phone itself.

For companies in regulated sectors, device-level controls are critical to ensuring that mobile phones and tablets with access to the enterprise network can be managed in a secure manner. With so many personally-owned devices and corporate assets on the network, IT organizations need a way to detect and identify devices, authenticate users and ensure that only authorized devices have access to enterprise applications and data.

Enterprises need to have a way to manage device configurations, provision applications and services, apply the right permissions and network settings and protect any business data that is stored on a mobile device. Often, all of this has to be done in a multi-platform environment, so any tools that the technology group uses for device management purposes have to support BlackBerry, Android, iOS and Windows Phone platforms.

In some ways, the goal of Mobile Device Management is to give IT groups the same kind of control over smartphones and tablets that they have over other corporate-owned technology assets. Not everyone agrees that this is a good thing. Workers using personal smartphones and tablets for business purposes, for instance, have resisted the idea of device-level controls that would give IT personnel access to their devices and the content on it. Some 84 percent of respondents in a survey conducted by Ovum cited privacy as their biggest concern in letting IT implement device-level controls. For others, it was fears of data loss and location tracking. Many users consider their mobile devices to be such an inherent part of their personal lives, they would refuse to participate in a corporate BYOD program if employers deployed certain controls on their smartphones or tablets. Some analysts, too, see overly restrictive device management as neutralizing some of the benefits of enterprise mobility.

Such concerns need to be factored in when implementing device-level controls. But ultimately, organizations in regulated industries have little choice. The risk of data loss from lost, stolen or misplaced mobile devices is far too great to be ignored or negotiated. Unless a company is willing to adopt a 100% Corporate-Owned, Business-Only (COBO) device policy, there is always going to be a need for controls at the device level. It's the technology group's choice how restrictive (or not) those controls should be, but at a minimum here is what every enterprise needs at the device level:

Password and Authentication Controls

A strong password should be a minimum requirement for any user wanting to connect a mobile device to the enterprise network. A mobile device that is not protected by a password or passcode puts any corporate data stored on the device at risk of unauthorized access and compromise. Unprotected phones and tablets can also potentially be used to gain access to any application or data to which the owner has

access. Enterprises must decide how strong they want device passwords to be based on their risk profile.

Configure devices to automatically lock out the user after a specific number of failed login attempts. If the data is critical, ensure device wipe in the event of multiple login failures. Appropriate policy controls have to be enabled to enforce the password requirement.

The goal of MDM is to give IT groups the same kind of **control over smartphones and tablets that they have over other corporate-owned technology assets**. Not everyone agrees that this is a good thing.

Local Encryption

One of the simplest ways to protect business data on mobile devices is to encrypt it. Use device encryption to protect application data, downloaded files, media data and other content on a mobile device. Encryption ensures that content is stored in a scrambled, unreadable form that can be reversed only with the appropriate PIN or passcode. Encryption ensures that even if the device is lost or stolen, the data itself is protected.

Most modern mobile operating systems offer native encryption support. Enable it and implement policies for ensuring that encryption remains enabled. Software encryption tools are available for organizations that only want to encrypt specific business data or files on the device and not all of the content on it. This is an approach that works best when other measures have been implemented to separate corporate data and applications from personal data.

Device Wipe

Enable remote device wipe capability on all mobile devices that access or store enterprise data. Lost, stolen and decommissioned mobile devices present a huge data loss risk for enterprises. In a survey conducted by Kaspersky Lab , roughly 16 percent of the respondents reported losing a smartphone or tablet or having it stolen. About 20 percent of the devices contained corporate data. Remote wipe capability ensures that all data and applications on a lost or compromised device, is permanently erased and the device is restored to its original factory settings. It offers the best assurance against data loss when a device goes missing.

Enterprises that want to avoid the liability implications of wiping personal data off a mobile device should use a Mobile Device Management tool to remove only company applications and data while retaining the user's personal data on the system.



Encourage users to take advantage of their device's native remote locate and wipe capabilities to get rid of sensitive personal data in the event their device gets lost or stolen. Insist that employees report any loss or theft of their mobile device to the IT organization as soon as possible in order to mitigate data loss.

Remote Locate and Remote Lock

IT organizations need to have the ability to quickly locate lost or stolen devices. Many modern smartphones and tablets support features that enable them to be tracked or locked down completely in the event they go missing. Enable these features to prevent a missing device from becoming the primary source of a data breach.

Application Whitelisting and Application Blacklisting

Use application whitelisting or application blacklisting techniques to restrict the applications that are allowed to run on mobile devices with access to the enterprise network. Both approaches are effective at mitigating security risks posed by malicious and poorly designed applications.

With whitelisting, the idea is to compile a list of applications that are approved for use on a mobile device and ensuring that mobile users can only download and use these applications on their devices. It is an effective way to ensure that only properly vetted applications can be downloaded and run on mobile devices that are used for business purposes.

IT organizations need to have the ability to quickly locate lost or stolen devices. **Many modern smartphones and tablets support features that enable them to be tracked or locked down completely in the event they go missing.**

Use whitelisting as a way to standardize the applications that run on a mobile device or group of mobile devices. Decide if you want an application to be downloaded mandatorily on a device or if you want it listed as an optional choice and use the appropriate device management tools to enforce the policy. The downside with whitelisting is that it can be too static and prevent mobile users from taking advantage of new applications quickly. So make sure the whitelist is dynamic and responsive to changing user needs and requirements. Otherwise, users will simply find a way around it.

Consider an application blacklist approach if you prefer giving users the ability to install applications of their choice so long as they avoid known bad applications. A blacklist

is less restrictive than a whitelist in that it allows employees to download and install any application on their device they choose so long as it is not on the list of banned applications. But its effectiveness depends entirely on the comprehensiveness of that list. If the blacklist is not constantly updated to reflect the latest malicious or risky applications, it does little to mitigate security threats.

Containerization

Separate business and personal data on a mobile device via containerization. Storing businesses data alongside personal data on a mobile device is risky. The applications that users download on a mobile device could

potentially pose a risk to enterprise data. “For example,” says BlackBerry ☞, “a voice recorder may store messages on a third-party server. Or a productivity app may access the user’s calendar. With the device being used for both personal and work tasks, it’s not just the user’s data that’s at risk,” but that of the organization as well.

Putting enterprise applications in a separate, software-defined zone or “container” on the device can mitigate the risk. IT can exercise its full range of control over the data and the applications in the container, while the mobile device owner is free to use the device for personal purposes. Several vendors of mobile device management products support containerization at the device operating system level.

Over-the-Air Programming and Configuration

One of the most critical requirements for any mobile device management strategy is the ability to manage mobile devices Over the Air (OTA) from a central place without ever needing physical access to them. OTA tools allow enterprises to keep an eye on devices on the enterprise network, enroll new devices, block unauthorized ones, configure them and to set or reset network permissions. OTA services allow network and security administrators to push out security notifications and updates and manage policy settings on both personally owned and corporate-issued mobile systems. An OTA capability is almost a prerequisite for mobile device management and needs to be a fundamental component of any enterprise mobility management strategy.



Segregating work and personal data on a mobile device – a technology called Containerization – can help ensure regulatory compliance.

Additional Controls

Several additional controls are available for organizations that want even more protection for mobile device use. For example, MDM tools are available that allow technology managers to restrict camera usage in an enterprise setting. Some tools prevent screenshots from being taken in the workplace; others limit the ability to copy and paste data on the clipboard, while some prevent data from being stored on removable media like the SD card of a smartphone.

All of these are useful controls to consider, especially for companies that manage sensitive data. For example, restricting a smartphone's ability to take photos in the workplace mitigates the risk of someone stealing data by simply taking pictures of it and storing it on the device.

Business Enablement

But as with all security controls, the key lies in finding the right balance between security and business needs. The more controls that are added on a mobile device, the more likely workers are going to try and find a way around it. Instead of approaching device management as a security or a compliance issue, the focus should be on secure business enablement instead.

Security controls need to be implemented as needed but they should be based on a thorough understanding of the risks.

Where possible, involve the mobile user in the device management process.

For example, much of the initial device enrollment and related processes can be made self-service. Instead of having users depend on the IT group to register their smartphone or tablet, enable a self-service

Over-the-Air capability is almost a prerequisite for mobile device management and needs to be a fundamental component of any enterprise mobility management strategy.

portal where they can do it themselves.

Consider allowing workers to use the portal not just for device registration purposes but also for configuring and managing their personal or corporate devices.

None of this can work, of course, without a strong usage policy governing the use of personal devices in the workplace. Engage and inform mobile users on how devices are provisioned and registered on the network

and on what data and applications are available to them via their mobile devices. Articulate clearly what they are permitted and not permitted to do with their devices and the policies that apply in the event a personal device containing business data is lost or misplaced. If “jailbroken” or “rooted” devices are not allowed on the network, state that explicitly to prevent future misunderstanding.

Instead of having users depend on the IT group to register their smartphone or tablet, enable a self-service portal where they can do it themselves.

CASE STUDY

UNIPRESALUD, SPAIN

Unipresalud is a Spain-based consultancy firm specializing in risk prevention and the improvement of workplace health and safety. The company has accreditation by Spain's National Labor Authority (Dirección General de Trabajo) to provide external occupational risk-prevention services, and has an 850-strong team of professional staff, and more than 120 service centers and 22 mobile units.

The Challenge

Unipresalud required a mobility solution to securely manage the exchange of corporate information among mobile workers. As its main activity relates to occupational health, Unipresalud regularly manages sensitive personal medical data protected by Spain's stringent Organic Law on Data Protection (LOPD).

The company's "service guarantee" required a robust mobility strategy to ensure the secure and confidential handling of medical information for corporate client employees, as well as the reliable management of its business processes.

Employees desired an intuitive user experience that simplified their ability to comply with the LOPD. Unipresalud's mobility solution also needed to be capable of securing Android™ and iOS devices that are used on its network."



The Solution

Unipresalud deployed BlackBerry 10 smartphones to regional managers, making it easier for them to communicate with each other through a secure mobile platform. Unipresalud also deployed BlackBerry Enterprise Service (BES) with Secure Work Space for iOS and Android to provide employees with iOS and Android devices with secure mobile access to corporate data.

"We have been using the BlackBerry solution for many years and we will continue to trust BlackBerry as our Enterprise Mobility Management (EMM) provider. BES is the best mobility platform for us in terms of integration, security, connectivity and price," said Xavier Albarracín Jiménez, CIO of Unipresalud.

Secure Work Space separates work from personal use by creating a secure and clearly differentiated work container for key business applications on Android and iOS smartphones. It leverages the same trusted behind-the-firewall connection available for BlackBerry smartphones and extends BlackBerry security capabilities for data-at-rest and data-in-transit to Android and iOS devices.

Unipresalud's Benefits

"The end-to-end encryption used on the BlackBerry 10 smartphones and BES ensures that information will remain confidential and uncompromised. Not only does BlackBerry's security help to prevent our data from being intercepted or hacked, it makes it easy for users to separate our employees' work email from their personal email," explained Xavier Albarracín Jiménez. "Working in separate environments where corporate data isn't available on the personal side can avoid costly mistakes."

The BlackBerry solution has been easy for the IT department to integrate with Unipresalud's "on premise" corporate email – making it

a robust, secure, reliable and easy-to-use solution. The team can also make updates remotely, which saves time and hassle for employees in the field. For those who use non-BlackBerry devices, Secure Work Space makes it possible to apply strong security settings to smartphones on Unipresalud's network.

The combination of BlackBerry 10 smartphones and BES gives the company an ideal combination of a flexible mobile management solution that meets both corporate and end-user requirements.

EXTREME MOBILE APPLICATION & CONTENT MANAGEMENT

Securing Mobile Apps and Content for Use in Regulated Sectors

Mobile Device Management best practices allow organizations to gain a critical degree of physical control over smartphones and tablets connecting to the enterprise network. But that by itself is not enough. Once a device has been successfully enrolled, it needs to have access to the right applications and tools for employees to be able to do their job. Users expect to be able to use their mobile devices to access, collaborate on and share business documents with others both inside and outside the enterprise network. This is where Mobile Application Management (MAM) and Mobile Content Management (MCM) practices come into the picture.

Securing Mobile Applications

If MDM is all about the device, MAM is about enabling central control over mobile application deployment and management. It's about giving IT groups a way to securely provision, update and monitor applications and application usage on corporate and personal smartphones and tablets. The focus is on application delivery and management based on factors like device type, operating system, user roles and access rights within the organization. Mobile application management software can help enterprises

tie applications and services to specific devices, users or user groups based on policy.

In theory, at least, mobile application management is not really very different from the processes that IT has used for years to centrally control and manage desktop and notebook applications and operating systems. But implementing these processes can be challenging in mobile environments — especially those that accommodate a mix of corporate- and personally-owned technologies.

Fortunately, numerous application management tools and services are available that allow enterprises in regulated sectors to take control of the mobile application environment without necessarily usurping control of the whole device. This is an important capability especially for organizations that have a mix of personal and corporate-issued systems. It is less important in an environment where all of the mobile devices are corporate-issued and therefore most likely under corporate control as well. But regardless of the mobile deployment model that is used, there are some application management capabilities that are critical, including the following.

Usage Policies

Any exercise in mobile application management has to begin with usage policies. This is a component of enterprise mobility that can be handled either as part of a device management strategy or as part of the application management strategy. Either way, the goal should be to have a set of clearly defined policies for device eligibility, role-based access and user rights.

It is the IT organization's responsibility to clearly spell out minimum security and configuration settings, and minimally acceptable device types and operating systems that can be used for running or accessing enterprise applications and data. As part of the process, organizations need to clearly define applications, services and portions of the corporate network that are available to mobile users. Employees should be given clear notice of their obligations when accessing enterprise applications with their personal mobile devices and be made aware of the need for IT to monitor the use of such applications on their devices.



Implementing mobile application management processes can be **challenging in mobile environments — especially those that accommodate a mix of corporate- and personally-owned technologies.**

Enterprise Application Stores

A dedicated enterprise application store provides a convenient and secure way to deliver enterprise-developed and third-party applications on a mobile device. Instead of pushing every application out to a smartphone or a tablet, in some cases it is more efficient to simply host all available enterprise mobile applications in one place and have users install them on an as-needed basis. Use an application directory or similar approach to list all the in-house and licensed third-party applications that are available to users from the enterprise app store, tailored to their specific roles in the organization. Users can choose the applications they require for their job from the list and directly install it from the app store.

It is IT's responsibility to clearly spell out minimum security and configuration settings, and minimally-acceptable device types and operating system.

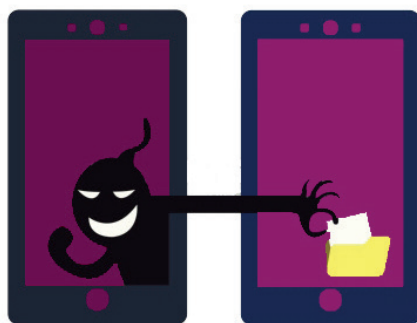
It's a good idea to include links in the application directory to consumer applications in public marketplaces like BlackBerry World and Google Play that have been vetted for use in the enterprise. Make sure that any volume discount codes, licensing or configuration information pertaining to these approved applications is pushed to the mobile devices as part of their profiles so users can take advantage of them when self-installing an approved consumer app.

Application Controls

Online marketplaces like BlackBerry World and Google Play give users a nearly limitless supply of applications over which IT has virtually no direct control. Many of these applications pose a danger to any enterprise data that is co-resident on the device not necessarily because they are malicious but simply by virtue of what they do. For example, a mobile application that allows users to copy data, record calls or backup content to the cloud could pose a risk to enterprise data.

Enterprise Grade File Sync and Sharing

Mobility managers who haven't already implemented enterprise grade services for content collaboration should make it a priority to do so.



The ease with which consumer services like Dropbox and Box have allowed individuals to share and collaborate with content, driving a growing interest in cloud file sync and sharing service among mobile users. A growing number of corporate workers have been using these services to store enterprise data and to collaborate on spreadsheets, presentations and critical business documents outside the enterprise firewall. The security risks posed by such use have driven many large organizations to explicitly prohibit the use of public file sync and share services. In a survey of 200 IT professionals conducted by Research Now on behalf of Ctera, some 55 percent forbid the use of such services while 71 percent expressed concern over data leaks and other security issues.

Despite such efforts, workers will continue to use such services unless organizations offer an enterprise-grade alternative for storing, accessing and sharing enterprise content securely. A growing number of companies have already implemented, or plan to implement, a private cloud storage service to address such needs. More than 25 percent of the respondents in the Ctera-commissioned survey, for example, said they had already implemented a private cloud sync and share capability while another 45 percent said they would do so soon. Where such services are not available or are explicitly banned, workers tend to simply use insecure email to share content on mobile devices.

Enterprises that want to ensure a secure way for employees to create, edit, and share content anywhere, anytime should implement a secure private alternative to consumer file sync and share services. Such a capability allows employers to push content securely to a central location and implement access controls for ensuring that only users with the proper permissions are collaborating with it.

As with other aspects of mobile security, organizations may sometimes treat content management needs as part of a device management strategy, while others may wrap it into the application management component.

Instead of pushing every app out to a smartphone or a tablet, it may be more efficient to simply host all available enterprise mobile applications in one place and have users install them as needed.

CASE STUDY

GLOBAL LEADER IN FINANCE

A leader in financial services, this company has thousands of employees distributed around the world. And given the round-the-clock nature of their industry, key players need anytime, anywhere access to critical applications, information and people.

The Challenge

When this company discussed moving to the latest BlackBerry smartphones, IT leaders considered what they'd need to do to transition their existing mobile apps to the new platform. At the top of their business-critical list: a custom, Java-based CRM and market data power tool that houses their critical pipeline, with hooks into email and calendars.

A Senior Enterprise Developer on the BlackBerry Enterprise Solutions Team explained that it was a matter of using one of the rich, standards-based development tools available for BlackBerry, like BlackBerry® WebWorks, or the BlackBerry® Native SDK.

Once the IT team understood their options, their next question was about timelines. Could they make an absolutely seamless transition quickly and efficiently? They'd take every precaution necessary, because even one unexpected application glitch, on one user's device, could end up slowing or sinking a massive opportunity. And because the app would contain sensitive customer data, it needed to continue to meet the world's toughest regulatory requirements, not to mention the company's strict internal security standards. The firm's internal application development specialists simply weren't in a position to shoulder that responsibility alone.

Fortunately, the end-to-end nature of a BlackBerry enterprise solution meant they knew exactly where to turn for support.

The Solution

"We started by understanding all the use-cases for the app — there were many — and then probing under the hood to see exactly what the transition would require," explains the lead developer on the BlackBerry Enterprise Solutions Team.

In order to enable the full BlackBerry user experience and performance, he recommended using Cascades™, and leveraging the special expertise of a BlackBerry application development partner. The BlackBerry Enterprise Solutions Team provided key insights on email and calendar integration.

The BlackBerry team was able to demonstrate how BES could help them manage the app through its lifecycle — to make sure it could continue to deliver as required when the company added new features, updated operating system software and deployed additional devices.



Key Benefits

- **One port of call:** BlackBerry app experts took on this migration issue, managing it in partnership with the customer, development partner and the account team.
- **The right connections:** After choosing the technology, advising on app architecture and design, and providing platform expertise, BlackBerry brought in a trusted partner to round out the development work.
- **The full picture:** While most mobility vendors provide a single piece of the puzzle, BlackBerry is the only EMM provider to address the whole picture, from devices to app development, and from technical support to Mobile Device Management and Mobile Application Management.
- **Future-proof apps:** Developed the right way from the start, BlackBerry apps are easily managed via the BES, and standards-based development frameworks make it easy to extend apps for multiplatform use.

Enterprises that want to ensure a secure way for employees to create, edit, and share content anywhere, anytime should implement a secure private alternative to consumer file sync and share services.

EXTREME MOBILE POLICY ENFORCEMENT

How the Right Policies and Data Analytics Can Ensure Proper Compliance

Devices that have been properly authenticated and enrolled on the network provide basic identity, device status and user profile information. That data is vital to registering the device on the network and for provisioning application access to individuals or groups of individuals. But the information by itself is not enough to enable true mobile policy enforcement for regulated companies that must comply with strict data protection standards.

Traditional policy control mechanisms do not work in a mobile environment. Smartphones, tablets and other mobile devices are unlike other corporate technology assets in that they can connect to the enterprise network or other networks anytime from anywhere via Wi-Fi and cellular protocols. Most have personal applications and data running on them that have not been approved or managed by the IT organization. Yet, at the same time, mobility managers need to be able to trust the devices enough to permit access to corporate applications and data.

For effective policy enforcement in such an environment, IT organizations need context awareness. In other words, access control and policy enforcement decisions have to be based on the context in which a mobile device is being used and not just on the physical attributes of the device or the user's role in the organization. This means having information on device and operating system health, the location from where a user might be seeking access, the type of applications and content being accessed, the security policies associated with the data and myriad other factors. To divine context, your corporate EMM solution must give you the ability to analyze the data collected to ensure your users are in compliance.

Inventory Mobile Devices

The best place to begin enabling this kind of a context-aware policy enforcement capability is with an inventory of all mobile devices that have access to, or carry regulated data. With the massive proliferation of mobile devices in the workplace over the last few years, it is vital for organizations to have a mobile inventory listing the prevalent mobile devices types,

operating systems and access methods used by employees to access corporate applications and data. Mobile devices based on BlackBerry, Android and iOS operating systems expose this data to configuration and inventory management software. So gathering and centralizing device and configuration data does not necessarily have to be an onerous task.

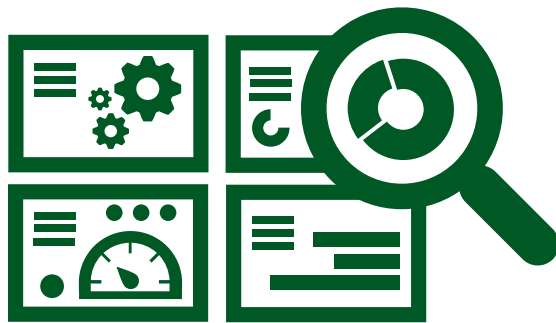
Maintaining an up-to-date mobile inventory can help organizations manage the lifecycle of corporate-owned mobile assets and keep track of personal smartphones and tablets in the enterprise. It allows IT managers to quickly identify devices that need a software update or security fix and to determine if the fixes have been properly deployed. A properly updated mobile inventory can also help from a compliance standpoint by giving IT managers some granular information on the types of devices connecting to the enterprise network.

Get a Handle on Regulated Data

Knowing what regulated data exists on mobile devices is vital to managing secure use of that data.

Slightly more than 70 percent of 798 IT managers polled by the Ponemon Institute ➤ in 2013 pointed to mobile devices as posing the single biggest threat to the security of regulated data. Yet, less than 20 percent had any idea of the extent of regulated data on mobile devices in their environment. Despite their stated security concerns, nearly 6 in 10 of the respondents said they allowed personal devices to access and store regulated data, while 43 percent said they permitted the data to also be backed up to cloud file sharing applications like Dropbox and Box.

Access control and policy enforcement decisions **have to be based on the context in which a mobile device is being used and not just on the physical attributes of the device or the user's role in the organization.**



Meanwhile, companies that did make an effort to scope the problem tended to rely heavily on non-scalable manual methods for identifying regulated data on mobile devices. Close to 40 percent of the respondents for instance, said they relied on manual monitoring of users to gather information on regulated data on their devices. A quarter said they used data leak prevention tools to get the information, while almost the same number used network monitoring tools. Not surprisingly, a majority of those polled felt that threats to regulated data on mobile devices were increasing and less than a third felt they were doing enough to mitigate the risk.

The numbers are a sobering reminder why enterprises need to have strong controls in place for assessing and inventorying regulated data on personal and corporate-owned mobile devices. Numerous surveys have shown the growing tendency among

mobile users to store business documents, spreadsheets, customer lists, financial information, and regulated data on their mobile devices, at great risk to their employers. Often, such data is backed up to a cloud file sharing service or sent outside the enterprise perimeter via insecure email applications.

In order to manage the issue, enterprises first need to have a clear understanding of the extent of regulated data on mobile devices. Automated scanning tools, including Data Leak Prevention (DLP) products and network monitoring tools, can help companies identify protected and regulated data such as Social Security numbers and financial information stored on mobile devices. Appropriate policy controls can then be applied on the device or the data based on the user's role and how and why the data is being used. For instance, by keeping track of data that is copied to or from a mobile device, or data that is shared via file sharing applications, IT managers can establish an audit trail for regulated data. If the usage is in violation of security policies, IT managers can enforce remedial action like locking further use, deleting the data or alerting the user.

From a compliance management perspective, having access to such information can be extremely useful for handling e-discovery requests. More than 65 percent of the companies in the Ponemon Institute survey said their organizations were subject to frequent or very frequent e-discovery requests. About 58 percent said such requests involved retrieval of regulated data stored on smartphones, tablets and other mobile devices.

Mobile users are **storing business documents, spreadsheets, customer lists, financial information, and regulated data on their mobile devices** at great risk to their employers.

Enable Location-Based Controls

Location-based controls are a fairly new approach to mobile policy enforcement. A location-based control is simply a policy enforcement mechanism that triggers certain responses when a mobile device enters or exits a predefined location or area, like an office campus, a building or sometimes even a room.

There are multiple reasons why an organization might want such a capability. Some government organizations and companies in regulated industries, for instance, have extremely strict requirements on where and how certain information can be accessed. The military, for example, might require that certain highly classified documents be only accessed from within the confines of a particular building or facility.

Or a business might require that a mobile device containing particularly sensitive business data never leave the facility. In other cases, an organization might just wish to disable certain mobile device functions like

the camera or voice recorder, or copy and paste when the mobile user is in a certain location like a meeting room or a laboratory.

From a security context, a location control basically establishes a way for enterprises to enforce specific policy restrictions on mobile devices while the devices are within the confines of a virtual area known as a “geo-fence”. Using such a control, an IT organization can configure a mobile device containing sensitive business data to generate an alarm if the device is removed from the building. Or, it could just as easily be configured to wipe sensitive data clean from the system if it is ever removed from a facility.

For marketers and retailers, meanwhile, technologies like geo-fencing and location-based controls offer a way to deliver new services and value-add to their customers. A retailer could use geo-fencing to serve up a coupon or deliver a promotional pitch whenever a mobile device owner is near the store.

Despite the positives, location-tracking tools need to be handled with care because of serious privacy concerns for employees. One major concern for personal device users is that a location control would allow employers access to detailed information on the mobile phone owner’s movements at all times. Enterprises need to be cognizant of the potential for violating an employee’s reasonable expectations to privacy when using such tools.

Enable a Centralized View

In order to manage policies across the entire mobile environment, enable a centralized view. A monitoring console or application dashboard should give IT managers a single place to view all applications in use and to sort the use by device and user IDs. It should allow a single unified view of all enrolled devices on the network and help identify any rogue devices that may be operating on it. Use the console to manage user

privileges, apply device-specific policy restrictions, enforce security policies, provision applications, push out updates and alerts, and to enroll or lock out rogue devices.

Take advantage of dashboards that offer IT managers a way to drill down into application use in order to troubleshoot performance issues and to set priorities for network use. With so many personal and corporate-owned devices competing for network resources, it is important to have a way to optimize use based on the user, the context, the data and the application.

From a security perspective, the management console should enable a view of all unauthorized access to restricted applications and give enterprise a way to monitor and audit such access. It should allow security managers and administrators to quickly generate reports of application and data use to meet compliance demands for such data.





In addition, enabling application-level policy controls can help enterprises optimize network resources. Because many mobile devices can run both corporate applications as well as consumer applications, enterprises need a way to identify and separate both in order to apply policy restrictions governing the use of each set of applications. For organizations that permit access to social media applications like Facebook, Twitter and YouTube, application-level controls help ensure that such use does not clog network resources.

Some EMM solutions can be configured to **collect and store detailed information about the devices connected to it** and how they have been used.

Data Analytics: Letting Your Data Tell Its Story

What if an organization is investigating an ethical problem like fraud and needs evidence of who was interacting with whom alongside the time and date of known events? Perhaps the event is a share price rising, key employees leaving, a robbery, a data breach, etc. Some EMM solutions can be configured to collect and store detailed information about the devices connected to it and how they have been used. Depending on the EMM and the device operating system, a time and date stamp can be captured for events such as phone calls, text and instant messaging, Web browsing, overseas travel, use of applications, unauthorized disabling of applications and security, jailbreaking or rooting devices, downloads and external transfer of files. Depending on the organization's employee and privacy rules, the technology exists to even track the network used and the location of devices on both GPS and cell-site coordinates.

Some illustrative examples of how analytics can be usefully applied to MDM/EMM server logging:

A bank under investigation that needs to produce evidence

The bank's CEO ignored the bank's security policy, which required all key employees to use secured smartphones. He insisted on using a device that did not enable logging of SMS and other user activities. Without this evidence, the senior executive would be unable to substantiate his version of events, leading to extensive reputational damage.

An investigation into fraud and insider collusion

A brokerage was continually losing its key talent to a rival firm. It suspected that a group of about 10 senior executives were colluding with the competitor to raid its best traders.

As soon as the executives knew that they were under suspicion, they all "lost" their smartphones. The brokerage did not have the required awareness or knowledge of analytics to access and use evidence from MDM/EMM logs.

An employee trying to abuse expense claims

An employee files an expense claim for a new tablet justified on the basis that it has been used for business applications. Based on logs from the MDM/EMM, it could be proved that no business applications had been loaded or used.



Given their compliance obligations, **regulated enterprises need to have a clear way to express and enforce mobile policy** and a way to enforce it effectively.

An IT service desk needing to trouble-shoot device problems

Mean time to repair (MTTR) can be reduced significantly when the IT service desk has appropriate information available for root-cause analysis. By capturing MDM/EMM log files, support staff are able to work faster and more effectively. For example, the logs may show that an application that is not working was loaded onto an antiquated or unsupported device or that a battery that is constantly being replaced is being drained by a specific application.

A disaster recovery scenario

An organization wants to audit and assess its response to either a real or simulated disaster recovery situation. Data assets from EMM platforms such as BlackBerry Enterprise Service can be used to assess how effectively communication and response has been handled over the incident timeline. Key performance indicators may include how successfully notifications and instructions were delivered and how effective subsequent communications (e.g., voice, SMS, BBM, IM, video, etc.) between responsible parties was in enabling successful execution of disaster recovery processes.

Risk management

An organization may be audited to assess how aware it is of risks and how well its documented controls are put into practice. For example, the UK Information Commissioner's Office (ICO), established to uphold information rights in the public domain, has found that many health care organizations are highly proficient at documenting and scoring risks and controls and completing risk registers, but can be ineffective at embedding those controls into their day-to-day operational practices. The logs from the MDM/EMM would enable a verification check based on risk-related data that is independent of how people subjectively assess and score their risks and controls. For example, perhaps a registered risk is compliance-related and concerns data protection laws, locally and globally. If the CIO scores the impact of a breach as high but the actual likelihood as low, it would be valuable to verify that assessment. MDM/EMM logs can indicate inappropriate use of file transfer applications, which files and websites have been accessed, and the list of files locally stored on the device.



Talent and competition

A business unit leader took a new job offer from a competitor and planned to take the best members of his team with him. Using SMS logs accessible via the MDM console, the company was able to prove that a breach of contract was in process and ensure compliance, thus preventing the exit of key talent from a high-value business unit.

For any enterprise mobility management strategy to be truly effective, regulated businesses need to have a way to set up and enforce policies pertaining to how, where, when and why users may access the network. It is a task that involves a thorough understanding of the devices and the operating systems in the mobile environment, as well as regulated data on mobile devices and flowing through the network.

Monitoring for Compliance

Given the compliance obligations that companies in regulated industries have to deal with, enterprises need to have a clear, effective way to express and enforce mobile policy. Automating and centralizing policy enforcement allows enterprises to maintain ongoing vigilance over the mobile environment. The actual enforcement component itself can be permissible or stringent, depending on the needs of each organization. For example, in some situations a policy violation may trigger only a warning or an alert notifying the use of non-compliance and urging remedial action. In other situations, an enterprise might take a more stringent action like removing or blocking a non-compliant application or forcing use of a mandating security control. In situations that merit such actions, the policy enforcement component can be used to delete or reset device data to prevent data loss.

CASE STUDY

VEPICA, LATIN AMERICA

Vepica is a global Engineering, Procurement and Construction (EPC) company with experience in a number of industries: oil, gas, chemical and petrochemical, power generation, and alternative energy. Over the past 40 years, Vepica has executed close to 3,500 projects in partnership with some of the globe's leading companies, most involving a great degree of technical complexity. Headquartered in Venezuela, the company has more than 2,000 employees worldwide, with offices in Canada, the United States, Mexico, Colombia, Peru and China.



The Challenge

With global demand for energy increasing, Vepica has ambitious growth plans. The company plans to increase their mobile workforce by more than 50 percent and therefore must have an easily-scalable solution for enterprise mobility management.

With a workforce spread out over four continents, this mobility solution also must provide employees with quick and easy – and secure – access to corporate information systems, while on the go. To support the large number of field operators in Vepica's remote locations, the company also needs a mobile solution that is device-agnostic and, above all, reliable and secure.

But scalability, flexibility and security aren't Vepica's only considerations. In most parts of the world, energy and chemical projects are tightly regulated and, to win business, Vepica must demonstrate it can meet and exceed any regulatory obligation.

"The company plans to apply international standard ISO 27001, which will certify information security management standards in our organization," explained Marianela Gil, Vepica's Vice President of IT.

The Solution

Vepica has relied on BlackBerry as a strategic partner in Venezuela since 2008 for mobile device management (MDM).

To meet its ambitious objectives, the company decided to upgrade to the latest BlackBerry Enterprise Service (BES) to support BlackBerry®, iOS® and Android™ devices.

The adoption of BES aligned very well with the company's latest IT policies and strategic infrastructure planning. Most importantly for Vepica was the opportunity to establish two separate environments on the devices, one for personal use and one for business where company data is secured by policies set by Vepica's IT administrator.

"One of the main reasons we chose the BlackBerry solution was the high level of security it offers for our mobile communications needs," said Gil. "BES gives us the flexibility to effectively and securely manage BlackBerry as well as iOS and Android devices. Additionally, the flexibility offered by the BES platform in terms of our corporate BYOD (Bring Your Own Device) policy added a lot of value at the time the decision was made."

One Platform, Many Benefits

The BES installation process is designed for ease of use and efficiency and provides Vepica with an optional set of extended IT policy settings, including corporate-only use of devices. It allows IT staff to, through a single console, deploy critical applications and services to all mobile devices, which can improve user productivity while maintaining system security. With BlackBerry® Balance™ technology, or Secure Works Space for iOS and Android™, the user experience can still be extremely rich in terms of apps in the personal space, without undermining corporate security policies in the workspace environment.

How It Works

- High-security standard and information protection on all devices, regardless of their operating system.
- Secure, reliable and seamless communications anywhere in the world.
- Provides collaborative opportunities for the workforce.
- Constant access to information for decision-making.



BlackBerry.com

IMPORTANT: Results provided for informational purposes only and will vary depending on the individual customer and the specific operating circumstances. This material, including all material incorporated by reference, is provided "AS IS" and "AS AVAILABLE" and without condition, endorsement, guarantee, representation or warranty of any kind by BlackBerry and BlackBerry assumes no responsibility for any typographical, technical, or other inaccuracies, errors or omissions in this material and shall not be liable for any type of damages related to this material or its use, or performance, or non-performance of any software, hardware, service, or any references to third-party sources of information, hardware or software, products or services.

©2015 BlackBerry Limited.