

# **Key Issues to Consider in Mobile Device Management**

**An Osterman Research White Paper**

*Published May 2011*

**SPONSORED BY**



**Osterman Research, Inc.**

P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA  
Tel: +1 253 630 5839 • Fax: +1 253 458 0934 • [info@ostermanresearch.com](mailto:info@ostermanresearch.com)  
[www.ostermanresearch.com](http://www.ostermanresearch.com) • [twitter.com/mosterman](https://twitter.com/mosterman)

## **Executive Summary**

---

The use of mobile devices – driven largely by smartphones and tablets – is growing by leaps and bounds. For example, worldwide shipments of smartphones during the fourth quarter of 2010 topped 100 million units, slightly ahead of personal computer shipments and 87% higher than mobile shipments for the corresponding period in 2009<sup>i</sup>. In-Stat forecasts that smartphone shipments will reach 850 million units by 2015<sup>ii</sup>. Tablet computer sales are experiencing similarly dramatic growth. For example, sales of Apple's iPad reached almost 15 million units by the end of 2010 – analyst firm Needham & Company estimates that iPad sales will reach 30 million units by the end of 2011 and 40 million by the end of 2012<sup>iii</sup>.

Mobile devices are increasingly used in the workplace, not only for tactical considerations like making access to email and the Web more convenient, but also for more strategic considerations that are focused on reducing overall corporate costs through telework. At the same time, however, mobile devices can create enormous compliance and management problems and require a new approach to ensuring that risks are mitigated and benefits from their use are maximized.

### **KEY TAKEAWAYS**

There are several important takeaways discussed in this white paper:

- The sheer number of mobile devices used in the workplace is increasing rapidly, as is the diversity of mobile platforms, operating systems and operating system versions. Also increasing is the variety of communication methods (email, Webmail, SMS text, instant messaging, social media, etc.) supported by mobile devices.
- Adding complexity to the management of mobile devices in the workplace is the fact that a growing number of personally owned devices are being used by employees alongside company-supplied devices. This is making mobile device management, in many ways, a shared responsibility between formal IT staff and the employees they serve – and creating risks and other problems as a result.
- Adding pressure to IT's mobile device management problem is the fact that these devices tend to be used by higher profile employees like senior executives and salespeople who are typically less tolerant of downtime when trying to access mobile email or other corporate resources.
- Moreover, the growing use of mobile devices means that a growing proportion of sensitive corporate data resides in employees' pockets, making access to and management of this data more difficult and more risky.
- In order to adequately manage the growing volume and diversity of mobile devices in the workplace, and to manage the growing proportion of corporate data that they contain for compliance and other purposes, mobile device management and archiving systems are an absolute necessity for organizations of all sizes.

## **ABOUT THIS WHITE PAPER**

This white paper focuses on the need to adequately manage mobile devices and data, as well as the risks that organizations face from the rapid growth of mobile device use in the workplace. It was sponsored by Notify – information on the company is provided at the end of this document.

## **Growth of the Mobile Device Market**

---

### **THE MOBILE DEVICE MARKET IS GROWING RAPIDLY**

The market for mobile devices is growing at a rapid pace. Consider the following statistics:

- IDC reports that mobile phone manufacturers shipped 101 million smartphones during the final three months of 2010, an 87% increase from Q4/2009. By contrast, IDC estimated that shipments of personal computers were 92 million during the fourth quarter of 2010, only 3% higher than for the corresponding period in 2009<sup>iv</sup>.
- Infinite Research estimates that shipments of “connected (cellular and/or Wi-Fi) consumer devices” will grow from 262 million units in 2010 to 712 million units by 2015<sup>v</sup>.
- In-Stat estimates that smartphone shipments will reach 850 million units by 2015. The company also estimated that smartphone shipments during Q3/2010 reached 81.1 million units, an increase of 89.5% from the same period in 2009<sup>vi</sup>.

### **THE NUMBER OF DIFFERENT PLATFORMS IS INCREASING**

Coinciding with the growth of mobile platforms is the growth in the number of different, major platforms in use. Major operating systems in use include Google Android (33% market share worldwide during Q4/2010<sup>vii</sup>), Symbian (31%), Apple iOS (16%), RIM BlackBerry (14%) and Windows Mobile/Phone (3%). Leading mobile phone manufacturers include Nokia (35.0% market share worldwide during Q1/2010<sup>viii</sup>), Samsung (20.6%), LG (8.6%), RIM (3.4%), Sony Ericsson (3.1%), Motorola (3.0%) and Apple (2.7%), among many others.

It is important to note that the tablet computing market is adding significantly to the diversity of mobile devices in use, particularly in the workplace. Apple, the current tablet market leader, sold nearly 15 million iPads by year-end 2010 and shipments of the iPad and iPad2 could reach 30 million by year-end 2011<sup>ix</sup>. One estimate already has 2011 shipments of the iPad at more than six million units in less than the first three months of the year<sup>x</sup>. IDC estimated the total worldwide tablet computer market at 18 million devices in 2010 and forecasts that shipments will reach 50 million in 2011<sup>xi</sup>.

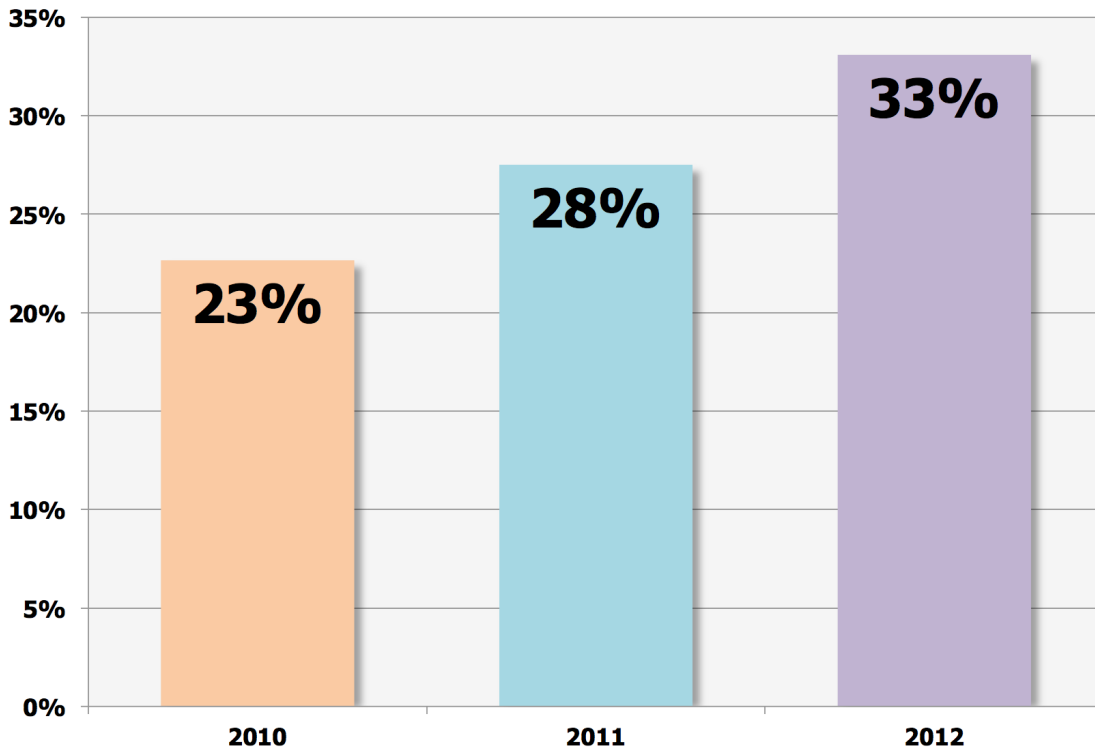
### **GROWING USE OF PERSONAL DEVICES IN THE WORKPLACE**

Mobile devices are being used increasingly in the workplace. Consider the following:

- Osterman Research found in a study conducted during December 2010 that 42% of the workforce in mid-sized and large organizations in North America uses a mobile messaging device at their place of work; this will increase to 48% in 2011 and 52% by 2012<sup>xii</sup>.

- This study found that 26% of employees were expected to be reachable on a personal (non-company-supplied or funded) mobile phone in 2010; 32% of employees will need to be reachable on their personal mobile phone by year-end 2011<sup>xiii</sup>. Further, a growing proportion of employees are voluntarily using their own mobile devices in a work context because of the flexibility in platform choice this affords them, and because many employers simply do not have budget available to purchase mobile devices for all of their employees. The State of California, for example, recently asked 48,000 state employees to return their state-owned mobile phones<sup>xiv</sup> as part of a cost-cutting effort.
- The same Osterman Research study found that company-supplied/funded smartphones were used by 23% of employees in 2010 and will increase to 33% by 2012<sup>xv</sup>, as shown below.

**Proportion of North American Employees Using Company-Supplied/Funded Smartphones**  
*2010-2012, Mid-Sized and Large Organizations*



### **MANY EMPLOY A MOBILE DEVICE**

Because of the rapid increase in the number of mobile devices in use – and smartphones in particular – it is no surprise that mobile devices are becoming the primary device used by a growing number of users, replacing desktops and laptops as the platform of choice while traveling, while working from home, and sometimes even in the office.

The growth in use of mobile devices is being driven in part by the increasing sophistication of the capabilities available on mobile platforms, as well as by improvements in processing power

in these devices. In turn, more capable mobile devices are enabling newer applications in a variety of industries, including financial services, insurance, energy, healthcare and other, often heavily regulated industries. Increasingly, mobile devices will replace the iconic desktop phone as the de facto communications tool for employees within the office.

### **WRESTLING WITH CORPORATE/PERSONAL DEVICE USE**

As personal mobile devices are used increasingly in the workplace, employers are struggling with the opposing demands that this use creates:

- An employee who chooses to use his or her own mobile device for work can save an employer a significant amount of money. For example, if an employer can avoid a \$200-300 mobile phone expense, coupled with avoidance of potentially \$2,000 or more in carrier fees and taxes over the three-year lifespan of the device, there is a temptation to do so – particularly during periods of strained IT budgets.
- However, use of personally owned and managed mobile devices in the workplace creates a number of problems and tradeoffs that IT and business decision makers must consider:
  - Smartphones contain a significant proportion of corporate data – an Osterman Research survey conducted in January 2011 found that 4.6% of corporate data is stored just on users’ smartphones<sup>xvi</sup>. While 4.6% may not sound like an enormous proportion of data, an organization with a total of just five terabytes of data under management will have 236 gigabytes of data on smartphones.

Employee-owned and controlled smartphones make access to this data much more difficult, such as during e-discovery, not only because of the difficulty that might be encountered in physically accessing these devices, but also because of the potential privacy and other legal issues that are raised by companies accessing their employees’ personal property.

- When these devices are used to access corporate resources, such as email or SharePoint databases, malware can be introduced into the corporate network given that most users do not employ any sort of defense on their mobile device. For example, a Trend Micro survey found that only 23% of smartphone owners employ the security capabilities that are installed on their devices<sup>xvii</sup>.
- It is also important to note that firms registered with FINRA and the SEC are required to archive and monitor communications via smartphone. For example, FINRA Regulatory Notice 07-59<sup>xviii</sup> states “...a firm should consider, prior to implementing new or different methods of communication, the impact on the firm’s supervisory system, particularly any updates or changes to the firm’s supervisory policies and procedures that might be necessary. In this way, firms can identify and timely address any issues that may accompany the adoption of new electronic communications technologies.”
- Personally owned and controlled mobile devices may also be more difficult to remotely wipe when lost or misplaced since they are not under IT’s direct control. This can expose corporate data to loss and may result in the breach of sensitive data, potentially triggering state, provincial or national data breach notification requirements.

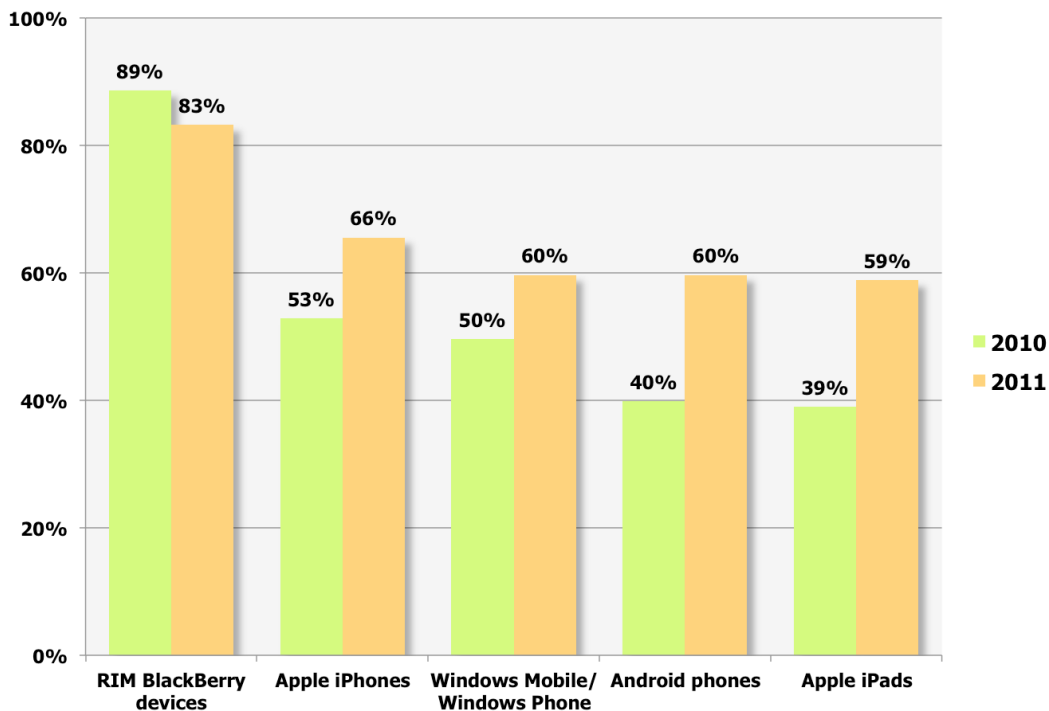
## Managing Mobile Devices is Difficult and Risky

Because few companies have just one mobile platform in use today, and because multiple devices must be managed and controlled efficiently in order to minimize out-of-pocket costs and IT staff time, supporting personal devices – and mobile platforms in general – is becoming more challenging and posing greater risks to organizations of all sizes. Over the near term, these challenges will manifest themselves in three key ways:

- **Platform growth will continue**

Virtually every analyst and other industry prognosticator agrees that the number of different mobile platforms in use in the typical organization will grow over time. As shown in the following figure, Osterman Research survey data supports this as well, showing rapidly growing support for newer platforms like the iPad and Android.

**Leading Mobile Platforms Supported in North American Mid-Sized and Large Organizations 2010-2011**



- **Mobile management will consume more of IT's time**

As a result of the growing diversity in mobile platforms and operating systems, IT will be increasingly focused on managing mobile devices, largely because many lack robust solutions that can efficiently manage cross-platform environments. The absence of these tools will force IT to spend an increasing proportion of their time on mobile management activities, resulting in less time available for other initiatives.

- **Corporate risk will increase**

The result of platform growth and increasing use of mobile devices for critical business applications will be an overall increase in the level of risk that organizations face. As more data is sent and stored on mobile devices, the level of compliance risk grows in several ways:

- Physical loss of devices increases the likelihood of a data breach, loss of intellectual property and related problems.
- The lack of archiving for mobile device content creates problems for organizations in the areas of e-discovery, regulatory compliance and overall employee productivity.
- Knowing what data is available on mobile devices becomes more difficult. This is particularly problematic for legal counsel and others that must assess the information that the organization has available to it during e-discovery, early case assessment and similar types of litigation-related activities.
- The growing number of devices accessing the corporate network – as well as home networks, Wi-Fi networks at Starbucks or McDonalds, etc. – increases the likelihood of malware entering the corporate network. This can result in data loss, financial loss and other negative consequences.

The bottom line is that organizations of all sizes must find a better and more efficient way to support and enforce corporate policy, manage mobile devices and to protect and archive the data on them.

## **Content Management for Mobile Devices is More Difficult Than for Traditional Platforms**

---

Content management for mobile devices – as well as management of the devices themselves – is more difficult than for traditional platforms like desktop computers and corporate servers. That makes mobile management more problematic, more time-consuming and potentially riskier.

### **IT OFTEN LACKS THE CONTROL THEY HAVE WITH TRADITIONAL INFRASTRUCTURE**

Unlike the traditional architecture with which IT staff is familiar, IT often lacks the control over mobile platforms than they have with the fixed infrastructure. By its very nature, mobile content management is more difficult, largely because the bulk of the infrastructure does not exist in a server room, but in employees' pockets and elsewhere outside of IT's direct control. This makes data more difficult to archive, content monitoring more problematic, and it makes legal and regulatory violations more likely.

However, despite the difficulties associated with managing content in a mobile infrastructure, the reasons to archive are identical:

- **Legal considerations**

Email and other electronic content stores – whether mobile or fixed – contain a growing proportion of business records that must be preserved for long periods of time. Further, this content is frequently requested during discovery proceedings and it must be produced more or less on demand. As a result, it is critical that all relevant electronic content be made available for e-discovery purposes.

Moreover, when data that might be required in a legal action must be held back from the normal deletion cycle, it is imperative that an organization immediately be able to retain all relevant data, such as all email sent from senior managers to specific individuals or clients, word processing documents that may contain corporate policy statements, spreadsheets with auditors' opinions, and so on. Placing a hold on mobile data may be more difficult than it is for traditional systems, but it is no less necessary.

- **Regulatory requirements**

There are a wide variety of statutory obligations to retain data, including the Health Insurance Portability and Accountability Act of 1996, public records laws, Securities and Exchange Commission rules, Financial Industry Regulatory Authority rules, the Sarbanes-Oxley Act of 2002 and literally thousands of other requirements that impose retention obligations on important business content, as discussed below.

### **MANY CONTENT TYPES MUST BE ARCHIVED**

Business records that must be retained for long periods can be generated by and stored in a large and growing number of systems: email systems, instant messaging systems, social media tools, collaboration systems, etc. However, the problem is complicated in the mobile realm by the need to preserve all of these types of content *plus* SMS/text messages – a content type that is not commonly employed in desktop environments.

Illustrating the growth of SMS/text messaging – albeit largely from the consumer realm – are statistics from the International Telecommunications Union indicating that 6.1 trillion text messages were sent worldwide in 2010, up more than four times from 1.5 trillion in 2009<sup>xix</sup>. In the United States, the CTIA estimates that 187.7 billion text messages were sent in December 2010 alone, up from 9.8 billion in December 2005 and only 14.4 million in December 2000<sup>xx</sup>.

Archiving of text messages – many of which contain business records that must be preserved for long periods – can be problematic for organizations and merits scrutiny while constructing corporate policy governing mobile devices.

### **KEY COMPLIANCE OBLIGATIONS**

There are a growing number of obligations with which virtually every organization must comply. These obligations, which are focused primarily on the archiving, encryption and monitoring of certain types of communications, include the following:

- The **Health Insurance Portability and Accountability Act (HIPAA)** requires healthcare and other organizations to protect sensitive health records of patients and others. However, the “new” HIPAA that takes effect during the first quarter of 2010 greatly expands the impact of the law. For example, while HIPAA previously applied mostly to physicians, medical practices, hospitals and the like, now the business associates of these

entities will be required to comply with HIPAA's rules about the security and privacy of protected health information (PHI). That means that accountants, benefits providers, attorneys and others that are given access to PHI will now be fully obligated to comply with HIPAA.

- Electronic recordkeeping rules established by the **SEC, FINRA, FSA** and other regulatory bodies are focused on financial services organizations' obligations to monitor and archive communications between registered firms and their customers.
- The **Federal Information Security Management Act of 2002 (FISMA)** requires the transparency of transactions and the types of information that must be captured when clients place trades. FISMA specifically requires instant messaging compliance by retaining conversations that reference trades.
- The **Federal Rules of Civil Procedure** obligate organizations to manage their data in such a way that their it can be produced in a timely and complete manner when necessary, such as during legal discovery proceedings.
- The **Sarbanes-Oxley Act of 2002** obligates all public companies and their auditors to retain relevant records like audit workpapers, memoranda, correspondence and electronic records – including email -- for a period of seven years.
- The **Payment Card Industry Data Security Standard** is a set of requirements for protecting the security of consumers' and others' payment account information. It includes requirements for building and maintaining a secure network, encrypting cardholder data when it is sent over public networks and assigning unique IDs to each individual that has access to cardholder information.
- The **Gramm-Leach-Bliley Act** requires financial institutions to protect sensitive information about individuals, including their names, addresses, and phone numbers; bank and credit card account numbers; income and credit histories; and Social Security numbers.
- **Federal Energy Regulatory Commission** Order No. 717 imposes various rules on regulated and vertically integrated utilities so that transmission providers do not give preferential treatment to their affiliated customers. The purpose of this order is to create an ethical wall between the marketing and transmission functions of vertically integrated companies that distribute electricity and natural gas between states.

In short, organizations face a variety of risks from their inability to properly manage, secure and archive the use of mobile devices in their organizations.

## **The Need to Focus on Policy Management**

---

Because mobile devices are more varied and more distributed than most other types of IT systems, they present challenges that are more serious and more difficult to address in terms of how policy management issues are addressed. Consequently, there are three important issues that organizations must consider:

- **There are different kinds of mobile data**

It's important to consider that "mobile data" consists of many different types of content that need to be managed in a granular way. For example, a mobile device can send, receive or generate email, Webmail, files, SMS/text messages, social media content, geolocation information and other types of data. For example, an email sent from a registered representative to a client, or an email sent by a company's senior manager to the company's internal legal counsel, will need to be archived. By contrast, a personal tweet or text message sent from the same device may not need to be supervised or archived in the same way.

Similarly, different devices may need to be managed in different ways: a company-supplied smartphone may be subject to a different set of regulatory, legal and best practice considerations than a personal iPad. However, it is important to note that even personal devices can be subject to strict supervisory and retention rules. For example, the FINRA Regulatory Notice noted above states that "FINRA expects members to prohibit, through policies and procedures, communications with the public for business purposes from employees' own electronic devices unless the member is capable of supervising, receiving and retaining such communications."

- **User behavior and training is key**

A key element in managing mobile device use is ensuring that users are adequately trained on their appropriate – and inappropriate – use. For example, users need to be trained on what types of messages can be sent from corporate and personal devices, how and when to send sensitive messages from mobile devices, the types of connections that are appropriate for sending and receiving content (e.g., a VPN to the corporate network when users are at home versus an unprotected Wi-Fi connection in a local coffee shop), etc. While Osterman Research has found that security technologies are somewhat more effective than user training in defending against data or security breaches, it is not a question of using one or the other: both are critical in protecting against security exploits and ensuring compliance.

- **Use a mobile device management platform to enforce policy**

Finally, it is important to use a mobile device management platform to enforce corporate policies and to back up user training. Such a platform is critical not only to manage the mobile devices themselves, but also to ensure that content is monitored, archived and otherwise managed in accordance with all required policies.

## **Important Considerations in Selecting a Mobile Device Management Platform**

---

When selecting a mobile device management platform, there are a number of important considerations that decision makers must consider. Of course, the importance of the following factors and the weighting given to them will vary based on the size of the company, the industries in which the organization participates, the number of mobile platforms used and other factors:

- **Create and enforce corporate mobile policies**

Any mobile device management system must be able to enforce corporate policies for both

corporate data/devices and personal data/devices. This is a critical consideration, since most organizations will have both corporate-sanctioned and personal devices in use, even if the latter are not officially approved by IT.

- **Simplicity and affordability**

Any mobile device management system must be simple for IT staff to manage, since IT does not want another time-consuming and complicated system to manage in addition to all of the other systems on which it must focus. Further, there is price pressure in this space, and so decision makers will naturally be sensitive to spending large amounts on either licensing or ongoing maintenance costs. This is of particular importance for smaller companies because they are spreading the cost of a mobile device management system over a smaller number of users, but large companies also wrestle with this issue.

- **Archiving all mobile content types**

It is essential that any mobile device management system integrate with the corporate archiving system so that business-critical content on smartphones can be archived in accordance with overall corporate policies for data retention. A failure to adequately archive mobile content can lead to charges of spoliation and create a variety of legal and regulatory problems.

- **Management of current and future devices and operating systems**

Any mobile management solution must be able to address current mobile platforms and operating systems, as well as those that might be deployed in the future. This is an especially important issue given the speed with which new devices can be adopted in the workplace, either with IT's blessing or simply through employee use of these devices in a work context. A key aspect of any mobile device management system is that it must be device-agnostic given the growing variety of mobile platforms finding their way into the workplace.

While some may balk at the "consumerization" of the corporate IT environment and may want to continue the old order of permitting only IT-deployed and sanctioned devices on the corporate network, the trend toward employee influence is growing. For example, an Osterman Research survey conducted in December 2010<sup>xxi</sup> found a variety of ways that mobile devices have been adopted in mid-sized and large organizations: in 54% of them individual users have purchased mobile devices and wanted to use them on the corporate network; an Osterman Research survey conducted 18 months earlier found that this figure was 45%<sup>xxii</sup>, indicating that employee influence on mobile platform choice is growing.

- **Flexible delivery options**

Organizations should also consider various delivery options for mobile device management: delivered either as on-premise systems or as cloud-based solutions.

- **Other considerations**

There are a number of other considerations on which decision makers should focus, including ease of use in order to minimize IT's involvement in managing mobile devices and to bring them up to speed quickly, and the ability to selectively wipe data (e.g., retaining corporate data while wiping personal data).

In addition, there are a couple of other important elements that can be important to consider when deciding on a mobile device management solution:

- **A centralized management console**

Particularly in environments with multiple mobile platforms, a centralized management console that will allow IT administrators to gain visibility into a variety of key parameters can provide significant value. Such a console can monitor and manage the devices on the network, the operating systems and versions currently in use, and key device parameters (battery level of each device, memory usage, roaming status, applications that have been installed on each device, etc.)

Further, the console can provide a breakdown of traffic, including the sites that users are visiting and the types of content that are being sent – the latter is particularly important for compliance purposes. Administrators can set thresholds and alerts, and have available to them location tracking for locating lost devices. Such a system can also allow administrators to plot, graph and extract data from the system database.

- **Self-service access for end users**

Mobile device management can also include a self-service portal to provide end-user access to basic capabilities without a 24x7 support function – this is a particularly important consideration for small companies that do not have an around-the-clock IT help desk. Capabilities that should be available to end users include the ability to remotely kill lost or misplaced mobile devices, the ability to lock devices, and the ability to locate devices if they are lost.

## Summary

---

Mobile devices in the workplace – both IT-sanctioned and personally owned devices – are proliferating because of the utility they provide and their larger role in enabling employees to be more productive when away from the office. However, mobile devices present unique IT and business management and archiving challenges. Organizations of all sizes and in all industries must deploy mobile device management systems that will enable devices to be managed properly, and that will archive content adequately.

## Sponsor of This White Paper

---

Notify Technology has been a solution provider in the wireless email market for over ten years. For six consecutive years, Notify has been recognized for their NotifyLink product by Gartner Group's Magic Quadrant for Wireless Email Synchronization. Notify has over 3,000 customers world-wide using its NotifyLink and NotifySync products.



**Notify Technology Corp.**  
**1054 South De Anza Blvd.**  
**Suite 202**  
**San Jose, CA 95129**

**+1 408 777 7930**  
**[www.notifycorp.com](http://www.notifycorp.com)**

Over the past 2 years, Notify has recognized the growing dilemma that exists for organizations and enterprises trying to manage the ever increasing number and type of mobile devices being used by their employees. CIOs and IT administrators in these organization and enterprises are realizing that they need more security, visibility, and control because of this diversity. In addition, since many of the devices are personally owned, the issue of control over business information versus personal information stored on the wireless device has become one of their top concerns to address.

Notify's recently released NotifyMDM product provides a single management platform capable of centralized command and control for all wireless devices regardless of platform. It is a simple, effective, and affordable mobile device management solution that provides IT professionals with the tools to manage and differentiate employee owned devices as well as corporate owned devices within the same enterprise or organization. NotifyMDM provides organizations and enterprises with unprecedented simplicity in centralized management and control of an array of wireless device platforms, such as Apple iOS, Android, BlackBerry, HP/Palm webOS, and Windows Mobile, Windows Phone 7 and select Nokia S60 Symbian wireless devices.

NotifyMDM is available as an On-Demand or On-Premise solution that will work with any email platform that supports ActiveSync including Novell GroupWise Data Synchronizer, Microsoft Exchange 2003/2007/2010, Microsoft On-Line BPOS. Office 365, and Live@edu, Lotus Domino Traveler, Axigen, Kerio, CommuniGate, Google Premier Apps, IceWarp, Ipswitch, Open-Xchange, Scalix, Zarafa, and Zimbra.

Notify has targeted the SME/SMB market with both an On-Premise and On-Demand MDM offering, however, the design of the NotifyMDM solution meets the requirements for large scale MDM implementations as well. Notify has leveraged its years of experience in the mobility market and has a proven track record of providing its customers with cost effective products, domestic based technical support, and an established business structure. Please visit [www.notifycorp.com](http://www.notifycorp.com) for more information on Notify's family of products.

© 2011 Osterman Research, Inc. All rights reserved.

No part of this document may be reproduced in any form by any means, nor may it be distributed without the permission of Osterman Research, Inc., nor may it be resold or distributed by any entity other than Osterman Research, Inc., without prior written authorization of Osterman Research, Inc.

Osterman Research, Inc. does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader's compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research, Inc. makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.

- 
- i <http://www.ft.com/cms/s/2/d96e3bd8-33ca-11e0-b1ed-00144feabdc0.html#axzz1I2CwxMAV>
  - ii <http://www.eweek.com/c/a/Mobile-and-Wireless/Smartphone-Shipments-to-Hit-850-Million-Units-by-2015-InStat-422416/>
  - iii <http://money.msn.com/top-stocks/post.aspx?post=9e199c32-1e92-4ba7-9ea1-122f8bbe8ba6>
  - iv <http://www.ft.com/cms/s/2/d96e3bd8-33ca-11e0-b1ed-00144feabdc0.html#axzz1I2CwxMAV>
  - v <http://www.connectedworldmag.com/latestNews.aspx?id=NEWS110308151745567>
  - vi <http://www.eweek.com/c/a/Mobile-and-Wireless/Smartphone-Shipments-to-Hit-850-Million-Units-by-2015-InStat-422416/>
  - vii <http://www.canalys.com/pr/2011/r20111013.html>
  - viii <http://www.gartner.com/it/page.jsp?id=1372013>
  - ix [http://www.thestreet.com/story/11064502/1/apple-ipad-sees-higher-analyst-estimates.html?cm\\_ven=GOOGLN](http://www.thestreet.com/story/11064502/1/apple-ipad-sees-higher-analyst-estimates.html?cm_ven=GOOGLN)
  - x [http://news.cnet.com/8301-13579\\_3-20048290-37.html](http://news.cnet.com/8301-13579_3-20048290-37.html)
  - xi <http://www.businessweek.com/ap/financialnews/D9LSJAVG1.htm>
  - xii *Mobile Messaging Market Trends, 2010-2013*, Osterman Research, Inc.
  - xiii *Mobile Messaging Market Trends, 2010-2013*, Osterman Research, Inc.
  - xiv <http://www.digitaltrends.com/mobile/california-to-eliminate-half-of-state-employees-cell-phones/>
  - xv *Mobile Messaging Market Trends, 2010-2013*, Osterman Research, Inc.
  - xvi *Content Archiving Market Trends, 2011-2014*, Osterman Research, Inc.
  - xvii Source: Trend Micro Inc. survey of 1,016 U.S. smartphone users, June 2009
  - xviii <http://www.finra.org/web/groups/industry/@ip/@reg/@notice/documents/notices/p037553.pdf>
  - xix <http://www.dhtech.com/how-many-text-messages-were-sent-in-2010/>
  - xx <http://www.ctia.org/advocacy/research/index.cfm/AID/10323>
  - xxi *Mobile Messaging Market Trends, 2010-2013*, Osterman Research, Inc.
  - xxii *Mobile Messaging Market Trends, 2009-2012*, Osterman Research, Inc.