



Consumerization

Managing the BYOD trend successfully

Employees dictate IT

Enterprises across the world are giving in to the “Consumerization” trend of employees bringing their personal mobile devices to work. “Giving in” has its advantages. For one, it will help enterprises reduce device and management costs. Secondly, it helps ensure employees are happier and more productive. On the flip side, as the Bring Your Own Device (BYOD) trend grows, it is likely to impact how IT support is provided and how enterprise data security is managed.

There are compelling reasons for embracing mobility and BYOD despite the challenges it poses. For the first time in history (in October 2011), said CTIA-The Wireless Association, the number of wireless

subscriber connections (322.9 million) had surpassed the population (315.5 million) in the United States and its territories. An IDC study released in January 2012 says that the world’s mobile worker population will reach 1.3 billion by 2015, representing 37.2% of the total workforce. Enterprises cannot afford to be slow in creating budgets, strategies, policies and processes to address this trend.

A Citrix study forecasts that by mid 2013, 94% of companies will have a BYOD policy. Gartner adds that by 2014, 90% of organizations will support corporate applications on devices owned by workers.

The Why, When and What of BYOD

BYOD as a phenomenon has been rising primarily due to the proliferation of smart devices and the consumerization of IT. The reasons enterprises are embracing BYOD include improved user experience and productivity, ability to have anytime, anywhere application and data availability and reduction in hardware procurement and management costs.

End User Trends Question: How do you manage this change?	
Then: PC Era	Now: Post PC Era
Traditional desktop form factors (laptops, desktops)	Compact and mobile devices (smartphones, tablets) share galloping
Largely location defined workforce	Distributed, decentralized and mobile workforce
Clear distinction between business-owned and personal devices	Line between business and personal devices blurring; employee owned devices being used for business
One organization - one platform; standardization	One organization - many platforms; flexibility

Dealing with complexity

As companies deal with the consumerization of mobile technology, the impact on the enterprise and on IT is overwhelming. Today, enterprises that have been driving standardization in IT for decades cannot afford to say they won't allow complexity within their IT environment. Added to this is the uncertainty over the evolution of mobility (see Figure 1 for the changes expected in platforms by 2015).

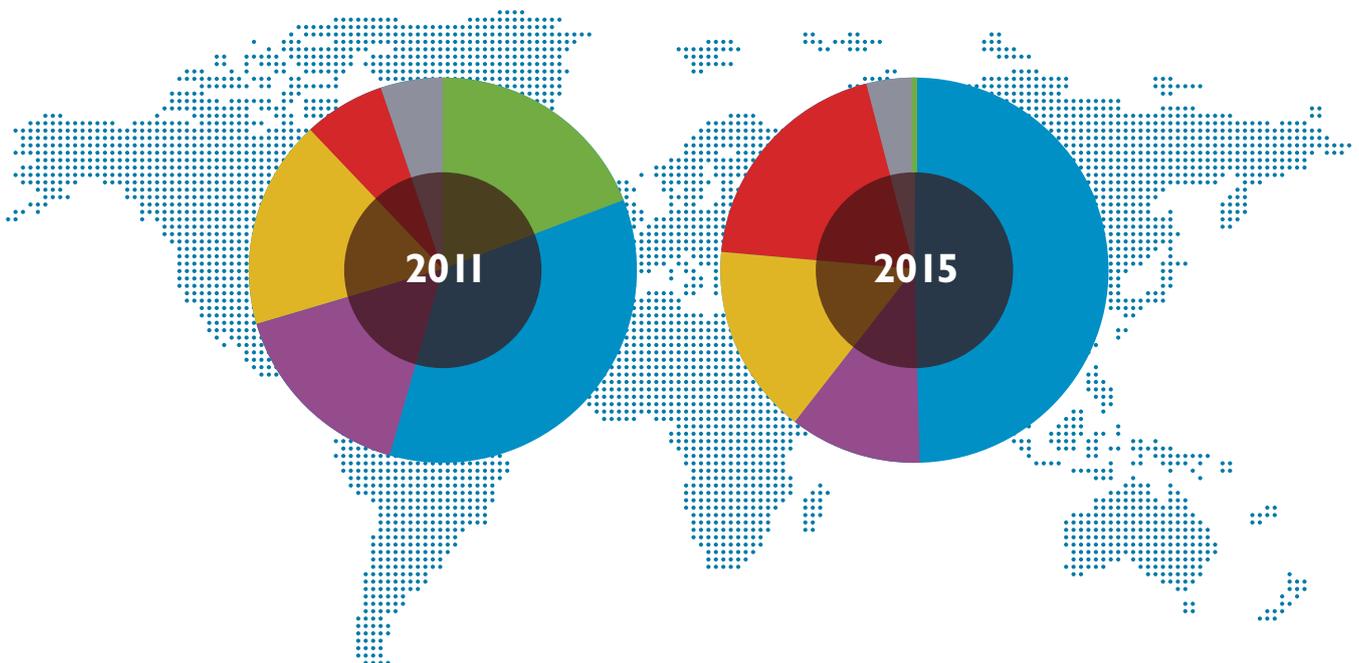
Trends shaping mobile app store strategy

Enterprises are hurrying to mobile enable their workforce. An increasing number of enterprises have invested in customized mobile

applications to ensure their teams are nimble and agile. A study by Kelton Research as far back as January 2011 showed that 21% of enterprises with a revenue of US\$ 100 million and above in the UK and the US were planning to release 20 or more mobile apps. Vendors like SAP, Sybase, Google, Oracle and Salesforce see 2012 as the year of mobile dominance. They are rolling out pre-packaged mobile applications that could be easy to customize, quick to deploy and will be cheaper than building and maintaining in-house apps. The acceleration in mobile enablement provides traction to the early stages of Enterprise App Stores adoption.

However, there are constraints on flexibility and scalability as business needs grow and technology matures.

**Worldwide Mobile Communications Device
Open* OS Sales to end users by OS**



	2011	2015
Symbian	19.2%	0.1%
Android	38.5%	48.8%
RIM	13.4%	11.1%
iOS	19.4%	17.2%
Microsoft	5.6%	19.5%
Others	3.9%	3.3%

Fig. 1 - Source: Gartner (April 2011)

*An open OS makes a Software Developer Kit (SDK) available to developers, who can use native Application Programming Interfaces (APIs) to write applications. The OS can, but does not have to be open source.

Amongst the challenges before enterprises are:

Multi platform device support: The expected shift in mobile platforms further emphasize the fact that it is unlikely that a single device/ platform or operating system will be dominant. As the mobile stack grows, IT departments will be forced to adapt to and support multiple devices. This means budgets will have to grow, coverage solutions created, hidden communications costs will have to be addressed and security issues dealt with.

Corporate data security: Data security is directly linked to device security. While it is relatively easy to observe security protocols and processes for wired networks, it is complex for mobile devices. For example, if the user loses the device, data is at risk. Should an enterprise have the ability to lock such a device or delete its contents remotely? Would this be permissible for what is essentially a private device? There are additional risks – such as threats from virus attacks and lack of sufficient encryption.

Network connectivity for these devices: Resource accessibility and network connectivity are perplexing issues for enterprises. Should personal mobile devices be allowed to access data, applications, mail and collaboration tools using the enterprise network, thereby posing a security risk? Should they be given access over a separate network? Bandwidth allocation and Quality of Service become critical, calling for new management tools. As an example, it is possible for IT to manually configure the wi-fi profile of a handful of mobile devices. Scaling this is difficult especially as employee numbers grow (and as employees exit) and types of devices grow. Enterprises adopting BYOD policies must think of the tools required to manage these technical challenges.

Device and usage monitoring: As the number of mobile devices that employees begin to use grows, enterprises will need to monitor device and usage. A user may have two or more devices logged into the network. Which one is personal? Which one is corporate? Device

registration and monitoring using MDM tools becomes critical. In a BYOD scenario, it is important to clearly define reimbursable costs else telecom expenses could burgeon out of control.

Application access: How should BYOD users access the various applications? Should they be able to download applications on their devices or should they access applications using virtual desktops or terminal services? What is the impact on the user experience? It is therefore important to clearly segment the applications and user profiles and accordingly craft out the application access strategy.

Theft, loss, and separation policy: BYOD solutions are not just technical in nature. They involve multiple functions like HR, finance and legal. It is important to have well defined agreements with employees to address the issue of what happens to corporate data when an employee separates or loses the device.

Device break fix and level of support for users: For what types of issues should the user call the Help desk? What sort of loaner policy should the enterprise have to address downtime of these devices? What sort of warranty should these users have for their devices? What sort of informal support groups can be created in the enterprise? While the device is personal, loss of device can impact business and productivity. An enterprise must define the level of support it will offer BYOD users and the expectations that it has from the BYOD users.

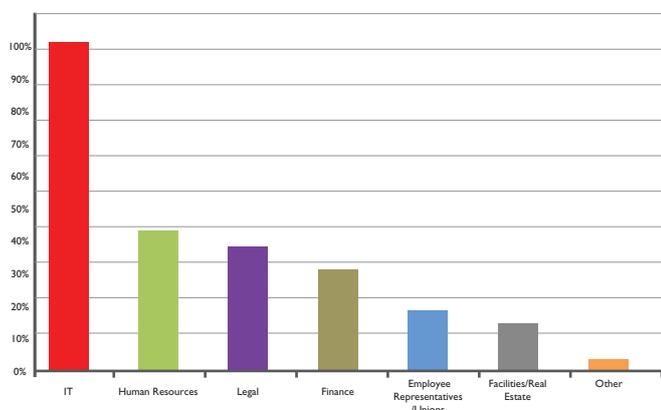
Compliance expectations from users: It is difficult for an enterprise to draw the line for policies and processes around BYOD solutions. For the enterprise, productivity, real-time capabilities and security will be the main concerns; users will continue to question enterprise processes that appear to curtail personal freedom. For example, issues like how often should passwords be changed and what is a strong password will have different answers from an enterprise point of view and device owner point of view.

BYOD Adoption Best Practice

The benefits of implementing a BYOD solution outstrip the challenges. To leverage the benefits, planning a BYOD strategy and solution begins with five steps:

Establish Policies & Processes: Multiple departments are involved in the creation of policies and processes (see Figure 2). HR will need to create policies for procurement of device and reimbursement of expenses; Legal will have to ensure that there is a clear understanding with employees with regard to data wipe, compliance and data privacy; Security becomes key with device registration and the definition of baseline security policies (device certificate based authentication, encryption, secure mobile gateway, password policy etc); and the enterprise must define the devices that are covered by the BYOD policy.

Departments involved in BYOD policies



Multiple departments are involved in BYOD decisions.

Fig.2 - Source: Citrix Global BYO Index, 2011

Implement technology solutions: Selecting the right technology to manage mobile computing platforms, networks and app access solutions can help keep enterprises secure and at the same time not compromise flexibility. These include having appropriate MDM, Network access, Security and Application access solutions.

Establish a mobility blueprint: During the process of embracing BYOD, it is important for enterprises to clearly define the business processes and applications that they would like to mobile enable and the roadmap for the same.

Establish an on-going support model: The model to support BYOD users needs to be defined. The existing Help desks could be leveraged. They will need to be trained on the level of support to be provided to these users. In addition, FAQs can be invaluable in addressing queries of the BYOD users with respect to the “do’s and don’ts” and the expectation from enterprise in supporting them. In addition, MDM tools can be leveraged to provide Asset Management, Device Management, Policy Management, Application Management and Expense Management services.

Start on boarding users: Once the above steps are addressed, the on boarding of users could start with communicating the finalized list of smart devices that employees can bring (no laissez faire), launch the pilot, roll out production and extend the platforms supported.

Taking a call

The suitability of a BYOD program needs to be decided on a case-by-case basis. This program may not be suitable for all class of enterprises. Scenarios where this program might not be appropriate include high security environments like military, research facilities with expensive equipment and valuable intellectual property and chaotic environments where audit and control enterprise software assets and data backup are not fully under control.

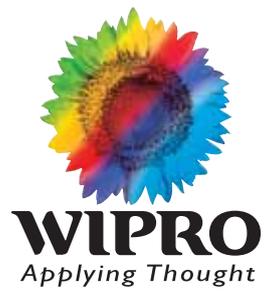
Consumerization of technology is for real and it is imperative for enterprises to recognize this trend and take proactive steps to embrace BYOD. At the same time there is a need to ensure that adequate safeguards are built into protecting the enterprise. It should not be an unbridled embracing of BYOD, rather it needs to be a well thought out and planned roll out.

About Wipro Technologies

Wipro Technologies, the global IT business of Wipro Limited (NYSE:WIT) is a leading Information Technology, Consulting and Outsourcing company, that delivers solutions to enable its clients do business better. Wipro Technologies delivers winning business outcomes through its deep industry experience and a 360° view of “Business through Technology” – helping clients create successful and adaptive businesses. A company recognized globally for its comprehensive portfolio of services, a practitioner’s approach to delivering innovation and an organization wide commitment to sustainability.

Wipro Technologies has 130,000 employees and clients across 54 countries.

For information visit www.wipro.com or mail info@wipro.com



DO BUSINESS BETTER

WWW.WIPRO.COM

NYSE:WIT | OVER 130,000 EMPLOYEES | 54 COUNTRIES | CONSULTING | SYSTEM INTEGRATION | OUTSOURCING

WIPRO TECHNOLOGIES, DODDAKANNELI, SARJAPUR ROAD, BANGALORE - 560 035, INDIA TEL : +91 (80) 2844 0011, FAX : +91 (80) 2844 0256, email : info@wipro.com

© Copyright 2011. Wipro Technologies. All rights reserved. No part of this document may be reproduced, stored in a retrieval system, transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without express written permission from Wipro Technologies. Specifications subject to change without notice. All other trademarks mentioned herein are the property of their respective owners. Specifications subject to change without notice.