



I D C V E N D O R S P O T L I G H T

Enterprising Mobility: Moving Beyond Bring Your Own Device

January 2012

Document number AU63203U

Sponsored by Telstra

The bring your own device (BYOD) discourse has dominated headlines and captured the attention of many Australian IT decision makers and executives over the past two years. However, there is a pressing need to move the BYOD discourse beyond the users and their preferred choice of device to a business conversation about enterprise mobility strategies that drive enhanced value and improved productivity. This IDC paper delivers the latest research on the evolution of the BYOD trend in Australia. It argues that CIOs and other IT decision makers can realise the perceived benefits of BYOD if they do so via a more holistic enterprise mobility strategy. One that involves the right policies, technology roadmaps and platforms, support levels, architecture and commercial models. Indeed, the many risks posed by BYOD can be mitigated with an enterprise mobility approach. However, considering the rapid pace of change in this mobile world and the breadth of disparate technologies underpinning its evolution IDC recommends CIOs and IT decision makers consider partnering with an external provider. This will allow them to leverage the provider's assets and capabilities while expediting the realisation of benefits.

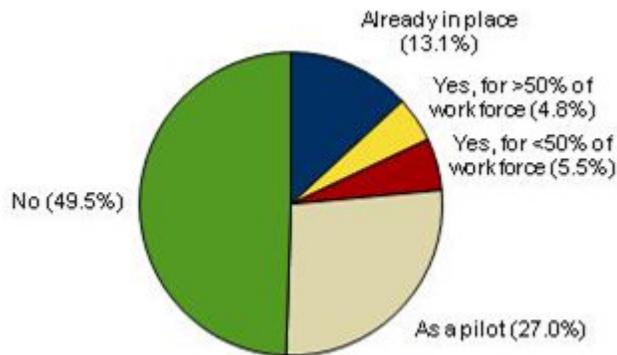
Why BYOD?

CIO and IT decision maker interest in BYOD has been stimulated by the rapid consumer adoption of smartphones and the exploding popularity of media tablets across Australia.

Figure 1

BYOD Intentions in the Next 18 Months

Q. Are you likely to enact a "bring your own device" policy in the next 18 months?



N=291
Source: IDC, 2011



The push by some employees, influential executives and tech savvy workers to use consumer devices for work purposes and IT department acceptance of this desire - officially or not - is a common circumstance in organisations of all types and sizes. It is one of many trends that is helping drive, and simultaneously be driven by the consumerisation of IT. This is a pivotal influence in many contemporary workspaces and one that IDC believes will play a significant role for many years to come.

As a result of this pressure and their popularity with senior executives, there is now an undeniable momentum toward adopting official BYOD strategies. IDC's Next Generation Workspace Ecosystem research¹ shows every second Australian organisation has some form of BYOD strategy on their agenda this year (Figure 1).

Perceived Benefits of BYOD

According to IDC research, the vast majority of CIO's and IT decision makers (73%) point to "increased user satisfaction" as the top perceived benefit of BYOD plans. This is an unsurprising result considering the perennial pressures IT departments face in meeting end user demands and the fact one of the main BYOD implementation drivers is pressure from end users for support of their consumer devices. The next top perceived benefits are:

- **Attracting and retaining a younger generation of employees:** 41% of CIO's and IT decision makers expect the adoption of a BYOD policy will result in the primary benefit of attracting and retaining a younger generation of workers.
- **Managing the work/life balance:** 37.2% expect BYOD to provide employees with better tools to manage this balance.
- **Collaboration, information sharing and flexibility:** 31.6% expect better employee collaboration, information sharing and flexibility from BYOD.

The Risks of BYOD

Whilst the perceived benefits listed above would certainly be welcomed by any organisation, IDC research has also shown there is a considerable level of risk present with BYOD that must be mitigated and managed. At the top of the list of risks is that of potential cost increases. Although there is also an expectation that BYOD strategies can reduce operational and capital expenditure by offloading the costs of device acquisition, maintenance and upgrades to the employee, IDC research indicates this may be unrealistic for many reasons. One of the main reasons is that only 19.3% of enterprise employees in Australia agree or strongly agree (Figure 2) that they would like to use their own device for work². In contrast, when asked in a separate question about their level of agreement to the statement that they would like the organisation to continue providing all their devices at work, 71% express agreement. Further, when asked again in another separate question if they were given an allowance to purchase a device would they like to bring their own, only 39% agree, and when asked if they would take responsibility for device maintenance, warranty and upgrades only 21% express agreement.

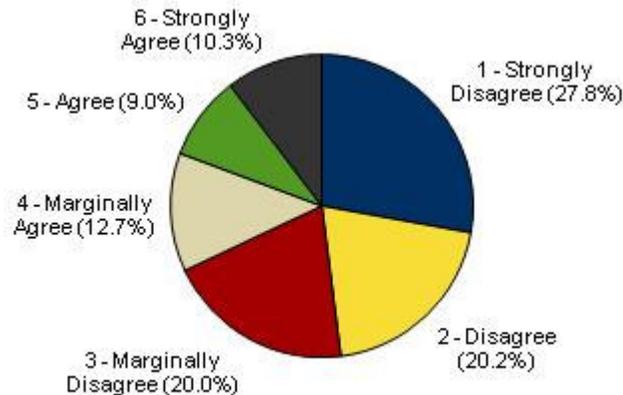
¹ *The Australia and New Zealand Next Generation Workspace Ecosystem CIO and IT Decision Maker Survey*, January 2012, By Trevor Clarke, IDC (Doc #AU1123706T on www.idc.com)

² *The ANZ Enterprise Employee Survey: Testing the Top 7 Assumptions about the Consumerisation of IT*, October 2011, By Trevor Clarke, IDC (Doc # AU1123701T on www.idc.com)

FIGURE 2

Enterprise Employee Support for BYOD

Q. Please indicate your level of agreement to the statement: "I want to use my own device for work and for personal use"



N = 600
Source: IDC, 2011

In short, this means if BYOD is implemented, IT departments will find it just as difficult to pass on the acquisition, maintenance and upgrade costs to employees as they have found it difficult to prevent rogue devices infiltrating the workspace. Indeed, if the goal of increasing end user satisfaction is to be achieved and the headaches of the consumerisation of IT reduced, it is likely IT departments will have to support both BYOD (which will involve a frequently changing range of device types and operating systems that have shorter lifecycles than typical enterprise grade models) *and* a traditional device provision model; in many cases both models for one employee. All of this equals additional costs. Other cost and performance factors that also need to be added to the risk equation of this likely workspace evolution include:

- **The requirement to ensure secure and anywhere, anytime access** to corporate applications and data for both organisation- and employee-liable devices. In a BYOD situation, this may result in multiple carriers with different network performance in terms of speed and latency. Ensuring an acceptable level of end user satisfaction and the performance of applications in these circumstances can become more complex than traditional models.
- **The ongoing provision of help desk support** for users with potentially unfamiliar devices and OS iterations along with the costs of ongoing training for help desk staff to provide this service. It is important to recognise that not all employees that want to participate in BYOD will be proficient at maintaining, upgrading or troubleshooting problems on their device and failure to assist them may mean lost productivity.
- **The ongoing management of the BYOD strategy** including: development and execution of accounting practices, especially for issues like determining reimbursement for personal versus business telephone and data costs; formulating and enforcing policies for the liability of commercial services that are procured such as carrier mobile broadband plans; formulating and enforcing policies around issues like users installing and purchasing their own line of business apps and also the ownership of data and intellectual property residing on a device; and updating

prescribed device catalogues to keep pace with popular consumer device launches to name but a few tasks.

- **The critical necessity of ensuring application compatibility and performance** across all devices and OS iterations. The current crop of consumer devices most likely to be used in a BYOD scenario span a highly diverse range of system specifications, form factors, brands, and operating systems that are more frequently superseded and upgraded than past enterprise devices. Implementing a BYOD strategy will necessitate a significant investment in talented staff to ensure applications are optimised and continually modernised for this complex and swiftly evolving world.

Whilst other factors may be added to this list it is clear that CIOs and IT decision makers will need to plan and manage any BYOD implementation carefully to avoid potential cost blow outs. Consequently this raises the question of whether organisations will have the internal skills and resources to effectively execute these strategies or if they would be better off seeking external assistance as part of a more holistic enterprise mobility strategy.

Why Consider an Enterprise Mobility Model?

IDC contends that a holistic enterprise mobility strategy that is part of a broader workspace vision and executed with the support of external partners will be key to implementing a BYOD strategy for most organisations in Australia. The introduction of significant change in the workspace such as BYOD plans will require long-term strategies for helping employees and the IT department adjust to new processes and approaches to how they complete their daily tasks. Because BYOD, if implemented in isolation, introduces a wide range of risks (and some benefits as outlined above) it is important that CIOs and IT decision makers are able to put together all the pieces of their workspace vision as efficiently and effectively as possible to realise the potential benefits. As such, it should be considered that an enterprise mobility model can be a fundamentally safer and a more holistic approach to enabling mobility in the workspace than BYOD can offer alone. The anywhere, anytime computing model is already a reality today that if ignored may mean a loss of competitive advantage. CIOs and IT decision makers should look to enterprise mobility models that offer state of the art architectures and network connectivity along with the following elements:

- **Capabilities to assess, plan, implement and provide on-going management flexibility.** The world of mobility is one of rapid change and innovation. Any enterprise mobility strategy should offer the means not just to get workers mobile, but also provide an agile vision and means for how this mobility will contribute to organisational goals and be managed effectively when it comes to the various policy development and execution obligations.
- **Device roadmaps that offer choice and flexibility.** The conspicuous absence of the element of choice from most organisations' device policies is one of the reasons many have suffered from an influx of rogue devices. Being able to offer end users a choice of devices that evolve with the organisation's expectations *and* user preferences will be vital to ensure existing consumerisation headaches aren't repeated in future. This should extend to all devices including smartphones, media tablets, notebooks and even desktops with additional monitors.
- **Proven mobile device management (MDM) platforms.** As the MDM market attracts vendor participants of varying quality and experience, CIOs and IT decision makers should be looking to those platforms that have proven performance through relevant case studies and reference customers, detailed roadmaps, and innovative technologies. These platforms, of course, must also be able to support BYOD strategies as part of the broader enterprise mobility vision.
- **Robust application development, modernisation and delivery.** Put simply, without the applications necessary to do their work, employees become liabilities and not assets. It is

therefore critical that in this emerging mobile world that comprises multiple OSs and devices (of varying form factors and specifications) that are frequently superseded and upgraded, that organisations are able to keep pace with the development of new apps or the modernisation of existing ones.

Profile of Telstra

Through its extensive experience with some of Australia's top enterprise and government customers, Telstra positions itself as a trusted advisor who can build a complete enterprise mobility strategy and architecture for customers. Telstra aims to do this by leveraging its strong relationships with application, service and device partners for an effective implementation with Telstra's Next G, Next IP and managed service offerings. As part of its approach to offering enterprise mobility Telstra lays claim to the following differentiators:

- **The fastest and largest mobile network in Australia.** Telstra operates the Next G mobile network, which has the broadest coverage in terms of geography and also the fastest speeds of any carrier in Australia. Additionally, Telstra has shown its commitment to its 4G network roadmap by investing in long term evolution (LTE) infrastructure across major capital cities and regional centres around the country.
- **Extensive relationships with key mobile device vendors.** Telstra maintains a device agnostic approach as part of its enterprise mobility offerings and has extensive relationships with most device manufacturers, including Apple, Samsung, HTC, Motorola, Nokia, BlackBerry, Sierra Wireless, and others. This device ecosystem is complemented by a certification system that identifies which mobile devices are recommended for use in rural regions that have Next G coverage; these devices are identified with a 'Blue Tick' symbol.
- **Proven MDM platforms.** Telstra offers the choice of the AirWatch or Mobile Iron MDM platforms. Both are proven vendors in the enterprise mobility space and are used by some of the largest organisations around the world. Additionally, Telstra offers a self-branded MDM platform for SMBs.
- **A comprehensive partner ecosystem.** In addition to its own internal solution architects, consultants and technology specialists, Telstra also maintains an extensive mobility partner ecosystem with over 140 partners that include some of the most well-known ICT vendors, application developers, system integrators and resellers operating in Australia.

To its advantage, Telstra has numerous enterprise mobility reference customers across a diverse range of industries that it can provide and is also able to draw on its deep set of assets and resources to assist customers with other ICT needs beyond enterprise mobility including, but not limited to, cloud computing and network services.

Challenges

For any service provider playing in the enterprise mobility market the challenge in the short term will be one of perception: can the service provider adequately support all of a given organisation's workspace needs? The CIO requirement for external service providers to assist with a broad range of workspace needs is one that consistently emerges in IDC's end user research. Considering strategies like enterprise mobility and BYOD are fundamentally intertwined with the workspace and how employees perform in their daily tasks it will be important for Telstra to effectively articulate to the market that it does have the required IT skills, services, partnerships and resources. IDC believes Telstra does have a strong offering in the enterprise mobility space so its challenge will be cutting through the noise and hype to show its true strengths.

Three Key Recommendations

It is still early days for the next wave of enterprise mobility and BYOD in Australia and as such IDC recommends CIOs and IT decision makers consider the following steps:

1. **Expedite the path to realising benefits by looking to an external enterprise mobility partner.** Focus on sitting down with a partner to understand how you can build a holistic enterprise mobility model that not only meets end user requirements, but also provides best practice (security, device management, application development and modernisation, policy development and execution, etc) under a commercial model that creates competitive advantage for the organisation. Anywhere, anytime computing is happening today and external providers can get it done now whilst most organisations do not of the resources or in-house capacity for the extra workload that enterprise mobility will bring. Expect a thorough assessment service from your service provider to ensure they have the right approach and capabilities. Look also to guaranteed outcomes and shared responsibility for success. IDC believes that as mobile devices, applications and OSs proliferate, and more and more organisations roll out enterprise mobility strategies but don't bring on additional IT employees, the need for external assistance will rise. These service providers will need to not only offer competitive pricing, but also be able to identify the unique imperatives of organisations and the vertical industries they operate in along with providing a broad set of solutions that place the employees and business outcomes at the heart of all strategies.
2. **Influence the influencers in your organisation and do it quickly.** As part of your enterprise mobility strategy you must ask whether all your staff really want BYOD? Or would Choose Your Own Device (CYOD) from a trusted provider be better? Unless strategies like BYOD are fully supported by the majority of employees in any given organisation, the deployment of such a policy may be simply problem shifting. That is, whilst addressing the problems created by the vocal and influential with a BYOD strategy, CIOs and IT decision makers may be unintentionally upsetting other employees that will one day vocalize their frustrations and dissatisfaction with workspace or device policies. Therefore, enterprise mobility policies that are flexible and accommodating of all parties' preferences are more likely to be successful. In other words, "choice" will be a defining characteristic of successful organisations in future and CIOs and IT decision makers should be seeding this idea as early as possible into mobility discussions with key influencers and decision makers.
3. **Measures for success.** By formulating robust success metrics, CIOs and IT decision makers will be able to measure the true value of BYOD deployment and provide return on investment justifications against the total cost of deployment to cost-conscious senior management. Many end user organisations do not have a clear picture of what it costs to provide ICT to different kinds of employees, nor how the introduction of new technologies will impact the organisation. Develop robust TCO profiles and look to peers and industry benchmarks to capture best practice around ROI metrics.

Conclusion

Whilst BYOD may be an attractive option for addressing the issues created by rogue devices and the consumerisation of IT, IDC believes that if adopted in isolation the risks may outweigh the benefits. However, if CIOs and IT decision makers go down an enterprise mobility path, they are more likely to mitigate these risks whilst still realising the best BYOD has to offer *and* the potentially powerful benefits that a mobile workforce can provide. To expedite the realisation of these benefits, CIOs and IT decision makers should consider an external partner that has the skills, assets and partnerships needed to formulate a successful long-term anywhere, anytime workspace strategy.

A B O U T T H I S P U B L I C A T I O N

This publication was produced by IDC Go-to-Market Services. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Go-to-Market Services makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

C O P Y R I G H T A N D R E S T R I C T I O N S

Any IDC information or reference to IDC that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC. For permission requests contact the GMS information line at 508-988-7610 or gms@idc.com. Translation and/or localization of this document requires an additional license from IDC.

For more information on IDC visit www.idc.com. For more information on IDC GMS visit www.idc.com/gms.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com