IDC VENDOR SPOTLIGHT

The Next Phase of BYOD - Improving Productivity by Managing Applications and Information on the Device

September 2013

By Dustin Kehoe

Sponsored by Telstra

The IDC Australia 2013 CxO Survey revealed that for the first time the top ICT priorities for business and IT leaders focus entirely on mobility. In order of priority the survey reveals that, CIOs are evaluating mobile device management and security, attempting to identify the right policy frameworks for Bring Your Own Device (BYOD), and embarking on a new mobile apps strategy for the future workspace. While this may on the surface seem to be three isolated projects, the reality is that they are not and must be supported by the same underlying architecture. Businesses are looking to build apps to engage customers, extend business processes to more devices, increase productivity among employees and lower the costs of their business operations.

This vendor spotlight highlights the evolution of the BYOD trend in terms of how IT organisations have been able to respond to the trend of employees bringing personally purchased devices into the workplace. What perhaps started as a reaction to the consumerisation of IT (CoIT) and the need to protect physical mobile end-points is evolving to the requirement to secure content, applications and information on an end-to-end basis from the corporate network to the mobile device. Once businesses have the management platforms to support the mobile workforce and security requirements, the next step for many is building apps at scale to drive competitive advantage.

Enterprises are clearly on a journey to extend apps from the enterprise to the mobile device. Underpinning this approach is a platform (or middleware) which allows developers to write apps once and deploy to any device and operating system. IDC defines this as Mobile Enterprise Application Platform (MEAP). MEAP is important for reducing integration costs to individual client devices, accelerating time to market for new apps and allowing IT to deploy and manage apps to scale. MEAP also provides IT and an application developer with the standard tools to navigate around thorny issues such as the trade-off between developing in HTML5 (which is important for availability and cross platform support) and native code. The latter is important for delivering a rich and interactive user experience. While there are many ways to offer a MEAP solution, IDC sees cloud as the fastest growing delivery model and one that is gaining wide user acceptance in Australia. In this context, cloud can also be referred to as Platform as a Service (PaaS) where application development and management is managed from a shared infrastructure.

The platform centric approaches are also helping businesses overcome some of the current challenges with BYOD by offering a stronger framework for data governance. This includes software development, distribution, licensing, user authentication and compliance through to maintenance, analytics and lifecycle management. This can help businesses to update apps faster, meet shorter delivery cycles where change management and continuous improvement are embedded in the development process. Agile methodologies are often synonymous with this approach.

IDC Australia Level 20, 8-20 Napier St, North Sydney NSW 2060 Australia P.61.2.9925.2298 F.61.2.9957.2330 http://www.anz.idc.asia

#AU63204W

Current State of BYOD

Formulating an IT Strategy

Employees are bringing their own devices into the workplace for business purposes. The practice is becoming the norm and will continue. IDC research shows that approximately 66% of businesses are embracing BYOD (in some form) and this is likely to increase in the foreseeable future. However there are some challenges ahead. The IDC 2013 BYOD Survey for Australia revealed that only 13% of businesses have a formal policy for BYOD. As a result, the majority of businesses and IT departments are supporting an uncontrolled BYOD. Amongst the 13% which are implementing a formal policy and IT strategy, not all businesses have been able to implement a successful BYOD strategy. There are a few reasons often cited for why BYOD can often fail the first time:

- **Data Security –** With BYOD, security is a major challenge and IT has often had to identify ways to separate the personal and corporate data on a device. This is often done through containerisation as well as identifying the right architecture to determine where the data or apps should reside (i.e., device, cloud and hybrid). There is also the need to set up usage policies and device management solutions should the device become lost or stolen. It has been difficult for IT in finding the right solution and in doing so walking the fine line of securing the device and gaining end user acceptance.

- **Data Privacy and Compliance –** With BYOD, there are also legal requirements which can limit the ability to deliver GPS tracking on devices which is important for determining if a device has been lost or stolen. Industries which are more heavily regulated may also come across additional requirements to comply with legal discovery and/or public disclosure. Even in cases where corporate data does not reside on the client, there can still be a requirement to turn in a physical device to meet a legal discovery obligation.

- **Employee vs. Corporate Liability –** A number of businesses have not been able to navigate through some of the key legal issues, such as establishing liability in cases where the device is lost, or data is infected with malware. With BYOD, there are other considerations if apps downloaded by an employee are in no breach of existing enterprise licensing agreements.

Whilst employees are finding value in using personally purchased devices for work purposes, it has been very difficult for IT to implement BYOD successfully and meeting all of the technical and legal requirements. We estimate less than half of the 13% of respondents that have implemented BYOD through a formal policy were successful the first time. IDC recommends that IT departments engage suppliers that are able to help design and build a BYOD framework. This should also be in consultation with lines of business, especially legal, finance and human resources.

BYOD: From Cost Savings to Productivity

Many organisations have reported short-term cost savings in BYOD by passing on the costs to employees. IDC has also reported in previous reports that short-term cost savings can often be overlooked with the long-term costs on IT resources in supporting BYOD, especially under an uncontrolled policy.

The real value in BYOD (when deployed correctly) can shift from tactical cost-savings to increasing employee productivity. This can be realised by giving the IT department the ability to support BYOD in a way that provides end-users the same access to applications, data and tool sets across any device. The content itself can also be updated in near real-time. Access rights can also be tied to employee roles, current locations or devices used at the time.

A number of businesses are treating screen sizes essentially as 'real estate.' In other words, IT is able to mobilise the workforce by providing the standard tools on every device which gives each

individual user access to the same documents, content, information and business apps based on their role. Every user is equipped with single log-in and standard interface. The number of use cases for building this type of solution is growing considerably in Australia as in other developed markets.

This approach for managing BYOD helps to avoid fragmentation both among devices (e.g., individual smartphones) and between them (e.g., media tablets, PCs, peripherals). Typically applications are written uniquely to a specific type of mobile devices and version of OS. While an individual user experience can be strong in one environment (e.g., iOS 5.0), it does not always extend to another. The knock-on effect would be great inconsistencies in delivering a strong end user experience that is uniform. This problem multiplies when IT is required to support a heterogeneous mobile estate. Given these trends, IT organisations will need to consider ways to reduce the costs and complexity while increasing the productivity of individual employees.

Productivity is gained by having employees access the same set of tools (data and applications) regardless of device and physical location. By 2015, 40% of workers will be mobile and spending two or more days of time away from the office each week in Australia. There will also be a sharp rise in workers that will not have an office as well as a modest increase in home-based mobile workers. Given that work is becoming more of an activity and less tied to a location, it is important for IT departments to identify the right sets of tools to support BYOD and encourage productivity. Mobile device management (MDM) is playing an important role for securing and managing data and end-points to enable BYOD while mitigating risks. There are a number of solutions on the market from data and device encryption, data containersation (separating personal and work personas), anti-malware, to secure e-mail and web browser capabilities as well as data loss prevention. Mobile security and device management will continue to be a requirement for business customers and a market that will continue to experience double digit growth over the next five years.

Mobile Application Management – From Devices to Platforms

As businesses are able to set up a security framework using MDM to match their unique requirements, the next stage in the mobile journey is around mobilising applications. Enterprises are looking to extend line of business apps to the mobile fleet. Customers are looking to engage mobile apps as a new digital channel over static web sites. Employees are embracing mobile apps to improve customer service or drive new efficiencies, such as replacing paper-based processes with end-to-end automation.

Mobile enterprise application platforms (MEAP) are at the core of delivering BYOD and supporting the enterprise mobile app strategy. Besides promoting productivity, organisations are also starting to build apps to improve business agility and customer interaction (mobile app is increasingly become a key channel for customers to find information and make purchases). MEAP extends the reach of existing enterprise applications and allows new apps to be deployed securely in the same environment. MEAPs enable businesses to meet the challenges of building apps faster and at a much lower cost base typically through a 'write once, deploy' model. MEAPs are offered both as an on-premise option and a cloud-based service with a per user/month licensing model. Many MEAP offerings include the platform, software development tools and front-end applications. IDC forecasts that the worldwide MEAP market will grow from A$2.1 billion in 2012 to nearly A$3.7 billion in 2015.

Mobile application platforms are central to the mobile apps strategy as they play an important role in allowing businesses to deploy mobile apps to scale. This is done typically by combining HTML5 – a browser based solution - which offers cross-platform support, lower development costs and wide availability with native apps. The latter delivers richness and strong user experience by integrating device resources such as camera, microphone and local storage into the app. Since native apps are tied to different source codes and OS's, delivering a consistent experience can be very costly.

A platform-based approach is important for delivering the best of both worlds while giving IT the necessary management tools. MEAP will be instrumental in enabling businesses to build and refine existing apps in faster update and delivery cycles where change management and continuous improvement are embedded in the development process. IDC forecasts that in 2016 the number of devices shipped each year (i.e., smartphones, tablets, laptops) will exceed the entire population of Australia. This will place enormous pressure on the IT organisation to keep up with the rate of change and proliferation of devices. MEAP give IT leaders the future proof assurance that it will be able to keep up with the shorter product lifecycles, accommodate new form factors and doing so in a secure matter which supports both customer preference and end user experience.

Profile of Telstra

As one of Australia's best known and largest companies with a long and successful history in telecommunications and information services, the Telstra brand needs no introduction. The company positions itself as being the only telecommunications carrier in Australia that can bring together all the components necessary for a successful enterprise mobility strategy, including mobile device and application management, mobile security and mobile app enablement. As part of its approach to offering enterprise mobility Telstra lays claim to the following differentiators:

- **The largest national mobile network in Australia** Telstra operates the Next G mobile network, which has consistently been proven to have the broadest coverage in terms of geography 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. 4G is an important consideration for delivering next gen apps at high speeds and offering capabilities, such as location-awareness, which is invaluable to some companies and a differentiator from pure WLAN environments. Many applications also need to work in real-time environment. Connectivity and high-speed low latency links in this context.

- **Investment in Mobile Enterprise Application Platforms.** Telstra has taken a A$18.3 million stake in Kony and it will be offering Kony's MEAP solution to customers. Kony solution offers a single code base with cross-platform APIs to support HTML5, hybrid and native code. This includes a full range of features such as security, audio and video integration, gestures, local storage and widget enhancements. Apps are built on platforms not individual devices. This reduces costs and offers scale for business to build apps once and to deploy across a myriad of device and operating systems. Kony's Enterprise Mobility Manager (EMM) also allows IT to centrally provision and manage apps, content, devices and users. Security policies can be imposed through a centralised interface to better protect apps, devices and data. Kony's acquisition of Sky Technologies bolstered the company's local presence and expertise in mobilsing back-end SAP environments. Kony's presence overseas can also benefit businesses with international requirements.

- **Proven mobile application enablement.** Telstra works with a number of providers to deploy innovative mobile apps for its business customers. Digitalinc (maker of ArisApp) has an extensive knowledge of business apps around content distribution and training materials. Other partners include Canvas which designs apps which increase productivity through the elimination on paper-based processes and GeoOp which offers workforce management solutions to services industries. Telstra partner apps are available on a monthly subscription through its T-Suite offering, enabling businesses to manage their mobile requirements through a single service supported with billing and provisioning. Telstra also works with AirWatch for MDM solutions.

- **Extensive relationships with key vendors.** Telstra maintains a best of breed approach to partners as part of its enterprise mobility offerings. This includes vendors such as Microsoft, Cisco, Citrix, VMWare and SAP. Telstra has relationships with most device manufacturers, including Apple, Samsung, HTC and BlackBerry. This provides the company also with insight into their solution roadmaps to better align with its customers.

- **Professional Services for Mobility.** Given the complexity of deploying BYOD and embarking on an app deployment strategy, Telstra offers consulting, solutions design and integration capabilities to support its customers. This is supported with an extensive mobility partner ecosystem that includes some of the most well-known ICT vendors, application developers, system integrators such as Accenture 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.

Future Outlook

Mobile device management is evolving from a point solution of securing and managing endpoints to addressing new requirements such as mobile app management (MAM) and mobile information management (MIM). Given the diversity of devices and operating systems, businesses will need to look for a platform based approach to deploy applications and manage data in a matter that is both secure and that provides a consistent user experience to any screen. Organisations will need to consider the following:

- **MDM vs. MEAP.** Mobile Device Management is an extremely important consideration for all areas around the security of the device, security of the data and setting the right policies around user experience. Adoption for MDM has been high in Australia and some vendors are extending the same management platforms and reporting capabilities to non-mobile devices such as laptops. Mobile Enterprise Application Platforms are critical for deploying apps to devices in a cost-effective and scalable way. MEAPs help to navigate complex trade-offs between browser based technologies and native code for delivering a strong end-user experience with mobile apps. The two technologies should be seen as the main pillars behind an enterprise mobility strategy and architecture.
- **HTML5 vs. Native Apps.** For a number of years, there has been a perceived trade-off between developing compelling feature rich apps which tend to be unique to every device and offers a strong user experience versus HTML5. Because the latter is web-based and it is widely available. Given the cost and complexity of client side support, most organisations will adopt hybrid deployments. Platform based approaches will be important for giving IT the balance between these two extremes at a price point that is affordable.
- **Growing Influence of Lines of Business (LOB):** IDC research has found that over 50% of ICT decisions are being influenced outside of the IT department. This number will grow to 80% in the next three years. LOBs will need to be involved in discussions around BYOD and mobile app deployments. Human resources, finance, legal and marketing will be important stakeholders in this discussion.
- **Rethinking Security:** Mobility is challenging all assumptions around security. As mobile apps are being deployed out in the field, many IT departments are reviewing perimeter-based security and role of the firewall. With proliferation of devices and mobile employees, security will need to also become context aware (e.g., device, location, user profile) and able to enforce consistent policy across fixed and wireless networks.

Conclusion

A recent survey found that 80% of businesses have a mobile app strategy or are developing one within the next 18 months. Some 15% of these respondents report that they are currently building mobile apps to scale (e.g., building apps in the 10s and 20s). Some 10% are looking to build apps to drive innovation and differentiation (e.g., establishing a B2C mobile channel). Among

businesses that have live deployments 43% of companies are using mobile apps to increase productivity and 37% use apps to support the LOBs. Nearly half of organisations also have an MDM solution in Australia and a further 40% plan to have one in place within the next 18 months. To support this rate of change, businesses are beginning to invest in technology platforms to the next gen mobile architecture.

BYOD has in many ways been a catalyst for this change. However, what started as a problem for how IT can 'reactively' support employee-owned devices coming into the business is now becoming a topic for how IT can 'proactively' put the right security frameworks in place with MDM while supporting the deployment of mobile apps and other tools to in increase employee productivity. These tools enable IT to provision and distribute the right application and data packages to employee groups by individual role and IT requirements. Employees can potentially benefit from stronger work/life balance to improve satisfaction in the workplace. Other IDC data shows employees want to choose their own device for work purposes. The IT department needs to manage all back-end issues such as authentication, compliance and lifecycle management in an automated way.

Mobile apps are also being used by some businesses to drive innovation and competitive advantage. One of the advantages with supporting mobility through a PaaS approach is to give IT the ability to deliver rich features (e.g., augmented reality, voice analytics and gesture) with the ubiquity of HTML5. The latter is to cut down the costs of client side development. This is carried out by offering a middleware which offers all of these capabilities from a single code base.

IDC recommends organisations consider the following when developing BYOD and building a mobile app strategy:

- **Not all apps are equal:** Mobile apps are needed for different objectives. App development, device and partner selection can vary as a result. For example the need to eliminate paper-based processes through online forms is likely to be advantageous to organisations which have large amounts of field workers (e.g., government, utilities, distribution, logistics, etc). HTML5 is often ideal for delivering these outcomes. However a retail chain may be looking to develop mobility as a channel for connecting with customers (alongside online and social media). These apps will require more feature richness and will need to access resources on the device itself such as camera, location and storage. While both can be supported from a platform approach, they will need completely different sets of specifications.

- **Understanding user requirements.** While mobile apps have been revenue generators for some companies and cost-cutters for others, business cases need to map to employee (or customer) requirements. IDC recommends that IT engages other stakeholders, such as LOB, and consider embedding resources. A process or transaction cannot be automated if it is not understood end to end. A successful deployment requires multiple inputs. Understanding user requirements is also an important input into developing the business case which is the make or break on most ICT projects.

- **Overcoming shortfalls with BYOD 1.0:** A platform based approach will be important for managing data and apps in a way where individual apps can be removed or added through a central platform, can be tailored to specific roles within a company and supported in a way that supports the growing complexities around building a successful BYOD strategy.

Asia/Pacific Headquarters: 80 Anson Road #38-00 Fuji Xerox Towers, Singapore 079907 P.65.6226.0330
F.65.6220.6116 www.idc.com