ovum

Practical considerations for your enterprise mobility strategy

Making BYOD and corporate-liable strategies work together

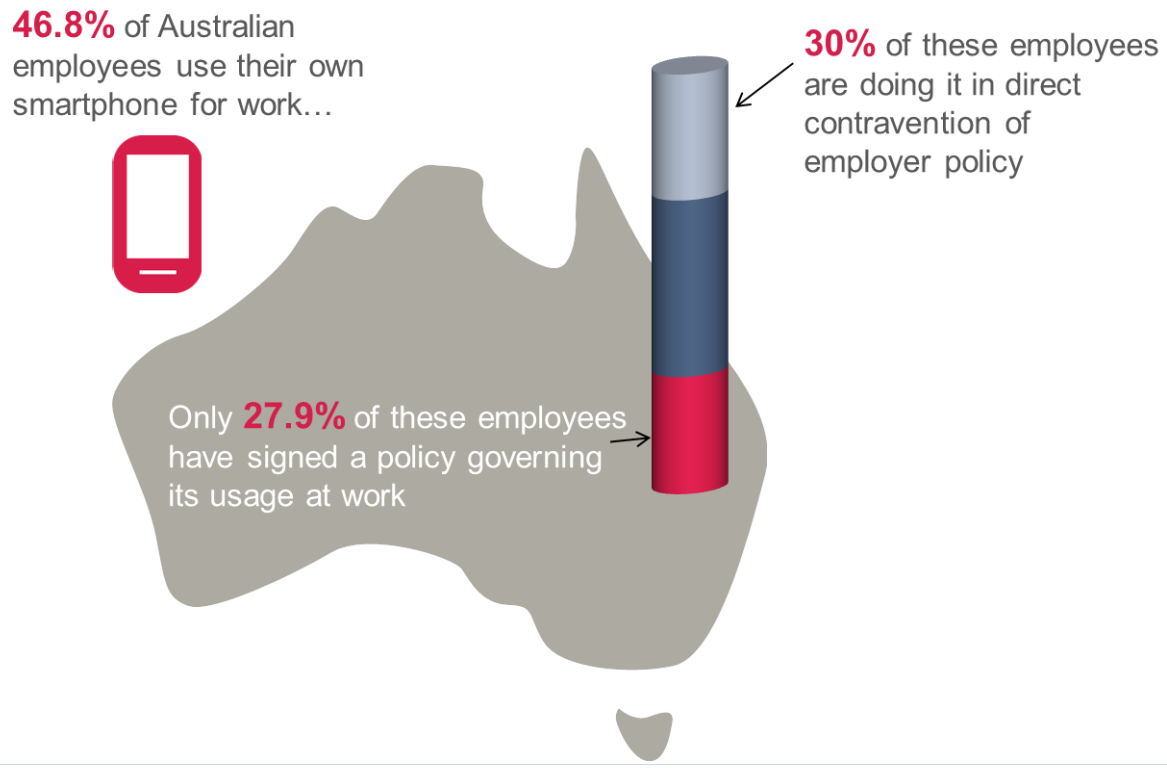
Summary

Introduction

The Bring Your Own Device (BYOD) trend continues to gather momentum. Ovum's research finds that the percentage of employees in Australia who use a personal smartphone or tablet for work grew from around 40% in 2012 to 51.5% in 2014. We define BYOD as a behaviour, not necessarily a strategy that businesses must adopt – it simply happens whether an enterprise IT department wants it to or not. There are various reasons why people do it, but the overriding theme is one of convenience and productivity. Employees want to use these devices, these "digital limbs" that are never more than an arm's reach away, to stay connected to work no matter where they are or what time it is. Businesses have an opportunity to improve the efficiency, productivity and potentially happiness of employees by embracing and harnessing this behaviour.

Ovum regularly talks to a wide variety of businesses across verticals and regions, and although the majority talk about implementing some kind of strategy or policy to manage BYOD, it is clear that it is still not being fully addressed. Consider the situation just around smartphones in Australia: 46.8% of employees use their own smartphone for work; around 30% of those employees do so directly against a stated corporate policy; and only 27.9% of them have signed a policy governing the usage of that device at work.

BYO smartphone in Australia: behaviour that still goes largely under the radar



Source: Ovum Employee Mobility Survey 2014, N=237

This trend is an important one for enterprise IT to address, and not just in terms of improving productivity and engagement: it presents immediate challenges and risks around data security. But it is also a difficult one to solve: from operating in a relatively homogeneous "comfort zone", IT is now

being asked to secure and manage data in a heterogeneous, multi-OS environment where each platform (primarily iOS, Android, Windows and BlackBerry) provides its own nuances and challenges. At the same time, for reasons of cost and privacy, IT needs to make the distinction between which devices are personally owned and which are corporate-liable. Almost half of Australian employees do not BYOD, and among those who do own devices but don't use them for work there are a couple of key factors holding them back: 36% want to keep their work and personal life separate, and 29% don't want their employer to have any kind of control over their personal devices. These workers will reasonably expect to have all the tools they need for work provided to them by their employer, so BYOD is unlikely to ever replace corporate-provided strategies – indeed in many cases it would not make sense to do so. In the majority of cases, therefore, any BYOD program will be complementary to a corporate-liable one.

Those tasked with defining and implementing a corporate mobility strategy must find a way to balance the two: segmenting the workforce to understand which approach is most appropriate in different cases, taking steps to secure data no matter what device it is being accessed on, giving employees access to the apps they need for work on whichever devices they use, separating out work and personal activity and data where necessary, and defining who pays for the hardware and data plans.

Key messages

- Corporate liable and BYOD strategies are complementary: BYOD cannot be ignored and there is a need to manage or directly enable this behaviour in many cases, while in other situations it makes sense to keep providing corporate devices.
- When implementing a mobility strategy, organisations need to first consider the needs of the employee and the business, segmenting the workforce to work out which mobility policy makes sense for which people.
- The organisation can then address key issues including data security, ensuring employee privacy, budget and expenses, technical support, and who the best service provider to work with is.

To BYOD or not to BYOD

When BYOD makes sense

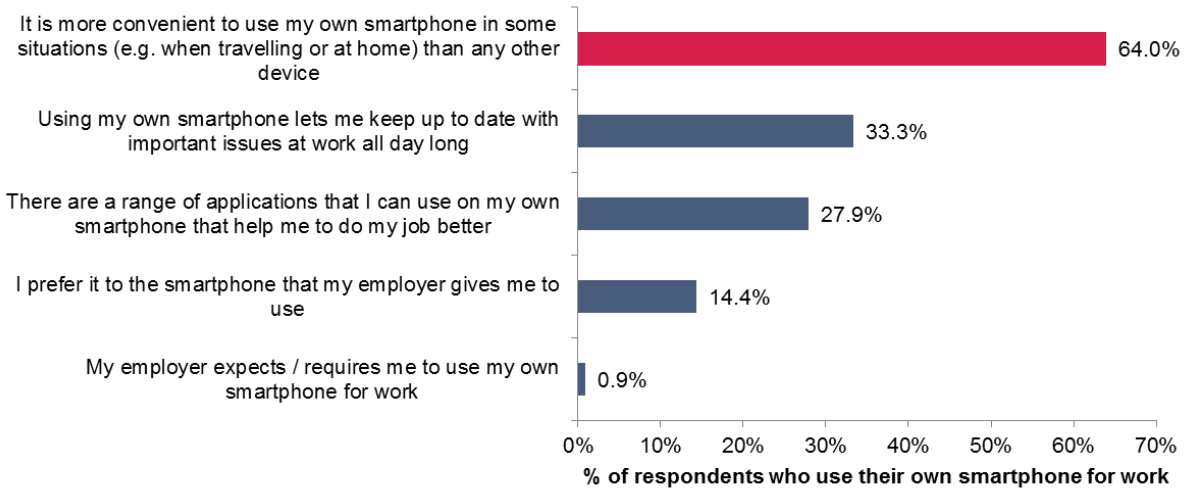
If an organisation is simply reacting to employee demand and keen to embrace the existing behaviour of its employees, then a BYOD policy will often make sense. As mentioned, 51.5% of Australian employees use their own devices to access corporate data in some context, and there is very little difference in that rate across verticals and job roles. So it is extremely likely that there will be a significant number of workers in every business that would like to be able to use their own devices.

Of course, meeting employee demand is not the only factor in play here. Workforce segmentation will also play a key role in determining whom it makes sense to allow usage of their own devices. For example if mobility is not key to the role of a particular employee but seen as more of a "nice to have" capability, providing them with limited access to apps and data on a personal device without covering any of the cost of that usage could be an attractive option. Enabling BYOD in this type of scenario opens up a range of potential productivity benefits. From simply providing access to mobile email to making a wider range of apps available, it means that a larger percentage of the workforce can be

productive while on the move than may be the case if the business only makes these apps available to those given corporate liable devices.

Embracing BYOD should not be seen as a cost-saving exercise (more detail on that later), but it can make sense where there is no expectation from employees that they receive reimbursement from their employer – i.e. where they are happy to use their own devices for pure convenience and because they think it will make their lives easier or improve career prospects. For many Australian employees, this sense of convenience rather than necessity is what drives them toward BYOD: 64% of those using their own smartphone for work say that they do so because it is simply more convenient in certain situations than using any other device.

Reasons why Australian employees use their own smartphones for work



Source: Ovum Employee Mobility Survey 2014, N=111

In any case, rolling out security and management software to all personal devices used by employees to access corporate data should be high on the agenda for businesses – whether those devices are only used occasionally or very regularly.

When corporate ownership makes sense

At the other end of the scale, if a job role is highly mobile and / or involves access to particularly sensitive data that requires a device to be locked down as much as possible, BYOD may not be the best option as it would require a significant amount of security and management measures that the employee may not want to see implemented on their own device. In these cases, some form of corporate provided device is likely to be a better option.

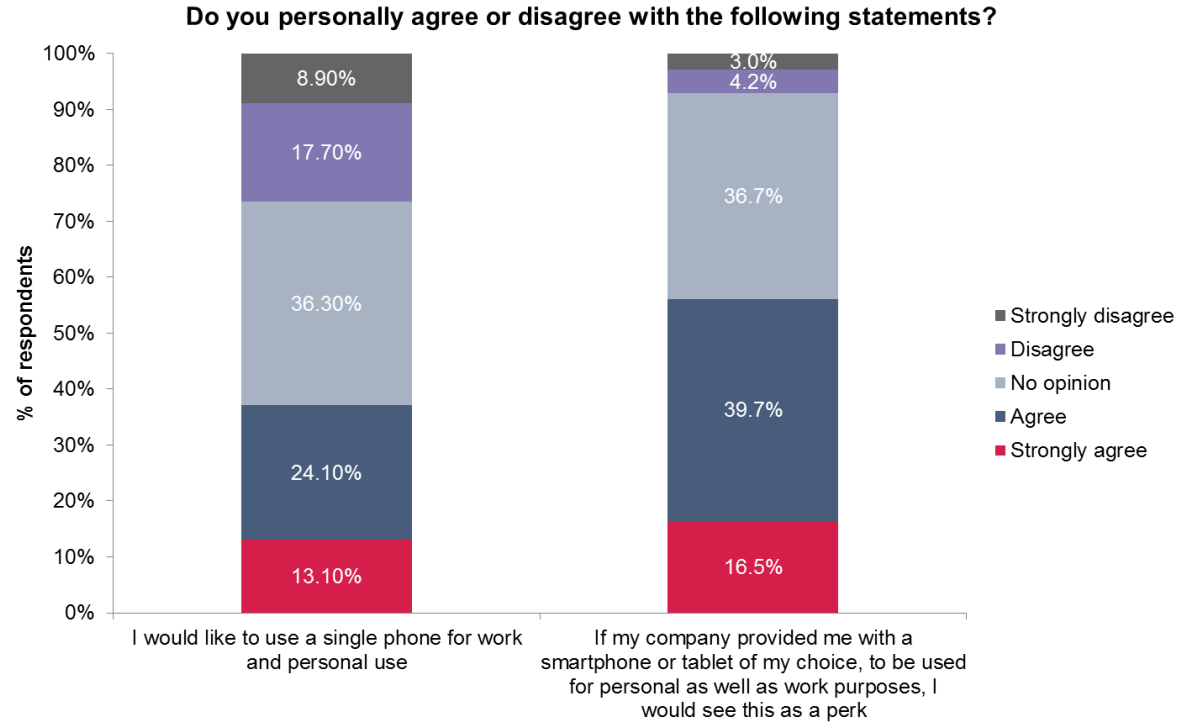
There are several potential ways to provide employees with corporate devices:

- Corporate owned business only (COBO): the employee is a given the device that the organisation wants them to have, for business use only;
- Choose your own device (CYOD): the employee can choose from a range of devices offered by the organisation;
- Corporate owned personally enabled (COPE): often going hand in hand with CYOD, the employee is provided with a device that can also be used as a personal device.

COBO deployments are best suited to environments where security and data protection is a key issue, and employees are very aware of the risks of data breaches and malware – for example in many defence, healthcare, or banking and financial services roles. This approach allows a business to lock down a device as much as it likes, without risking concerns over the need to manage multiple platforms. Such lack of choice may still be a problem however if employees have a preference for a particular device or operating system and are not comfortable using the device chosen by their employer.

In many ways, a CYOD / COPE combination is a good middle ground between BYOD and COBO. This approach can offer employees a similar choice over device and platform that they would get when buying a personal device, but still give the employer leeway to easily install the required security and management software. It also addresses one of the key drivers of BYOD behaviour: around 37% of Australian employees state that they would prefer to use a single device for both work and personal purposes; COPE allows them to do that. And 52% would consider it a perk to be given a device that could be used for personal as well as work purposes, again indicating that a COPE strategy would go down well with a lot of people.

Australian employee attitudes to single device usage and COPE



Source: Ovum Employee Mobility Survey 2014, N=237

Corporate-liable models also allow businesses to keep a better track on mobile spending. There will be a greater upfront cost around hardware than against a non-stipend funded BYOD model, but corporate negotiated voice and data plans can be far more economical than reimbursing individual personal plans.

Practical next steps for balancing corporate liable and BYOD strategies

Segmenting the workforce to understand employee and business needs

The first step in any enterprise mobility strategy is to get a good handle on what is already going on inside the business. As a consumer driven trend, we often find that IT departments don't appreciate the scale of BYOD behaviour going on within the wider organisation. This is of course easier said than done: obtaining direct and honest feedback from employees may be a challenge especially in cases where individuals feel that disclosing their behaviour might put them at a disadvantage or even risk losing their job. So, establishing this baseline is likely to be a focused project in itself, and quite possibly require the assistance of specialist consultants to find out what devices and apps people are using, why they use them, and what they'd like to be able to use. This first step can kick start the process of segmenting the workforce, identifying who should be BYOD-enabled and for whom it makes more sense to provide a corporate liable device.

Another part of that segmentation exercise, and the key to eventual success in terms of any mobile deployment, is gaining an understanding of all the business processes that could be improved or transformed through mobility. Different tasks are likely to require different types of devices: for instance if you needed an administrator to get simple access to mobile email it could quite easily be set up on their personal smartphone (should they wish to use their own device); while a field engineer may need access to some quite specialized apps on a 4G connected, ruggedized tablet, which is more likely to be a corporate-liable scenario.

Identifying all of these processes is tricky, and is an on-going job. There is no way that any enterprise IT department can have insight into every single line of business process or pain point, so communication between lines of business and IT is vital. Building a cross-business Mobile Centre of Excellence or a Digital team is a good way of bridging this gap between IT and lines of business; popularizing the push towards mobility across the organisation and feeding ideas into IT. At the same time, IT can use it to educate people about best practice around mobility, especially in relation to data security.

Securing data on all devices and apps

Once a strategic direction has been identified, and decisions made over which users are BYOD-enabled and which are given corporate liable devices, the first key issue to address is data security. It is often hard to tell exactly where a leak begins, but the proliferation of devices now accessing corporate data opens up a myriad of new opportunities for data breaches and cyber-attacks, which can be hugely costly in reputational as well as revenue terms. The Australian government's Cyber Security Centre (ACSC) identified 11,073 cyber security incidents affecting Australian businesses in 2014, at an estimated cost of AU$1bn.

BYOD behaviour is of course a particular concern in this respect: if left unmanaged, an organisation will not be able to keep track of where its data is or who's using it, or protect against malware. The three key vectors for any security breach are through the network, endpoint and application; and simply put, BYOD greatly increases the risk by increasing the number of networks, endpoints and applications that are used to access and process corporate data. BYOD exposes a business to the

risks inherent in unsecured consumer devices that were not designed with the enterprise in mind. For example, BYOD means that Android's dominant market share in the consumer space is spilling into the enterprise – and upwards of 95% of Android devices are potentially vulnerable to the Stagefright bug. Stagefright is only one example of thousands of bugs and pieces of malware in the Android ecosystem that enterprises need to protect against.

Implementing appropriate security measures across all types of devices and apps enabled by the business is therefore vital. At this point, the workforce segmentation exercise again comes into play and policies should be set according to the risk profile of each employee. For example, a junior employee without access to any sensitive data is unlikely to require the same level of authentication and security on their device as a board level executive. The main challenge for IT departments is providing the right security features across all the different mobile OSs and devices – most do not have the resources or skills to handle this heterogeneous environment internally. For this reason, the enterprise mobility management (EMM) market has been booming, with software vendors providing cross-platform management and security.

At the basic level, this means providing mobile device management (MDM) features such as PIN enforcement, device encryption, remote lock and wipe, and activity logging. Mobile security should also be included as part of a holistic security strategy, of course, including network security and identity and access management (IAM). But different security approaches will suit different mobile scenarios: Full MDM is appropriate in corporate liable deployments, for example, but a more flexible, customised, lighter touch approach to MDM may be better suited to BYOD deployments where a full device lockdown is not necessary. Employees can be wary of having a client installed on a personal device that has the capability to monitor all their personal activity and wipe personal data. In that case, or in a COPE scenario, a containerized solution that separates work and personal data, securing and managing only the "work" persona on the device, could be a better fit. In either case, the most important factor is to ensure policy governance across all corporate apps and data.

Ensuring employee privacy in BYOD and COPE implementations

At the same time as protecting corporate and sensitive client data, organisations are also legally bound to protect the privacy of their employees. Data privacy legislation differs between countries and sometimes between verticals, but one key right is present in every region that Ovum has examined: individuals must give explicit and fully informed consent for their personal data to be accessed or controlled. This is highly relevant to BYOD and COPE management: installing a software client on a personal device that is able to monitor personal activity and wipe personal data constitutes access and control of that individual's data.

Employees should therefore be made fully aware of the implications of corporate mobility policy and any management software installed on their personal devices, including which applications will be monitored and/or be eligible to be wiped in the event of the loss of device or the employee leaving the organisation. Employees should then give explicit consent for any security or access solution (such as an MDM client or corporate app store) to be installed on their device.

Even if the security solution is configured to completely ignore personal data and applications (such as a container), it is a good idea to ensure that the employee understands, accepts, and agrees with this policy, and to still require consent to deploy the solution. This may protect the company from any future allegations by disgruntled employees that they did not know what they were signing up for. Of

course, if the employer claims that it will not encroach on personal data, it must ensure that it does not do so in practice.

Budgeting and expenses

As with any enterprise technology rollout, costs around the preferred enterprise mobility policy need to be considered. When BYOD first took hold, many organisations jumped at it as an opportunity to cut costs – but while BYOD may offer some savings on hardware, this approach can be a little short sighted. Firstly, the cost of the EMM or endpoint protection software and services needed to manage and secure the data on the device can add up quickly – and of course these costs apply for corporate liable devices as well. Secondly, and specifically on the BYOD side, reimbursing employees for work usage on their personal voice and data plans can be far more expensive than paying for the same usage on a corporate negotiated plan. Australian businesses providing stipends to cover personal mobile costs are paying and average between AU$140 and AU$270 per employee upfront for the hardware, and then a further AU$40 to AU$70 per month per employee for voice and data plans.

This is an area that organisations may look to their mobile service provider to help with, finding favourable rates or extra services for employees who use their own devices for work and alleviating complex processes of reimbursement. Examples of carriers providing such services include AT&T Work in the US, and Telstra in Australia which provides a fixed cost option for BYOD that also includes security and management software and enterprise-level support.

Questions to answer in terms of budgeting for BYOD include:

- Who pays for the hardware, the employee or the business?
- Who pays for air time and data connection, the employee or the business?
- If the business is paying for the hardware and / or the wireless connection, how will this be addressed: via expenses? Through a stipend?
- Should a hybrid approach be considered, such as letting the employee bring the hardware but supplying a corporate SIM, or using a solution that allows for multiple numbers to run on a single SIM?
- What are the costs involved in either supporting this policy in-house or bringing in a third-party EMM solution?

Technical support and service management

Managing the new generation mobile estate in-house will be difficult for most organisations, as it requires expertise on the service desk across multiple operating systems, and granular policy setting according to employee profile: what data they have access to, what type of devices they use, whether their device is personally or corporate-owned. In a BYOD deployment in particular, organisations will need to address the following questions:

- Who is responsible for technical support: the IT desk or the individual?
- Will users be responsible for some applications and/or services while IT is responsible for others? If so, which?
- To what extent are users expected to keep their devices up to date with the latest patches, OS upgrades, etc.? Will the IT desk offer support in upgrading employee-liable devices if asked?

To provide solutions to all these issues (as well of course as data security) and take the pressure of the helpdesk, enterprises are looking to EMM software and managed mobility services. Outsourcing device delivery and replacement, voice and data plan management, and device and app management is likely to be the most efficient way of securing and maintaining any large scale mobile deployment. The supply-side managed mobility space is highly competitive, but is also relatively immature and potentially confusing market for businesses to navigate. Nevertheless it is highly important for organisations to find service providers that best suit their particular needs.

Finding the right provider: what to look for

Given all the choices discussed so far – the segmentation of the workforce, the balance of corporate liable and BYOD policies, the different types of device and app enabled, the different EMM solutions available, the different policies set to individuals and groups, the different ways of reimbursing employees, the different helpdesk policies – every enterprise mobility strategy is unique to the organisation and the choices that it makes. There is a large selection of software vendors vying for business in the EMM market, aiming to help manage various aspects of the strategy and solving particular problems. But, given the relative immaturity of the market, there is no single vendor that yet meets every possible enterprise requirement. Some are very strong in terms of security and MDM, but lack features around app management or telecoms expense management (TEM). Others might provide a robust TEM solution, but no containerization. And some might provide better support for one or two mobile OSs, but not for others.

Carriers and managed service providers are therefore in a good position to provide end-to-end managed mobility services. They can partner with best of breed software vendors in each area of EMM, offering a more complete end-to-end solution that could be tailored to the specific requirements of the business – for example a container solution for those on BYOD or CYOD / COPE schemes, MDM for those on COBO, corporate voice and data plans for all, and continuous helpdesk support and device and app lifecycle management. They can also provide wireless access and SLA guarantees, and support across this integrated set of services. If all performs as it should, this complete approach suits the needs of employees as well as the enterprise IT department.

Mobility strategy: basic next steps checklist

Mobility strategy: actions	
Employee behavior understood	✓
Workforce segmented	✓
Business processes identified for mobilization	✓
Candidates for corporate liable and BYO devices identified	✓
Security and management software in place	✓
Security policies set according to user / device type	✓
Work and personal data separated where necessary	✓
Calculations made and policy set on reimbursement	✓
Technical support and service responsibilities outlined	✓
Service provider support in place	✓

Source: Ovum

Given the practical considerations for BYOD, there is considerable value to be found in consulting with technical experts so that the most appropriate enterprise mobility strategy with BYOD and corporate-liable strategies working together is followed.

Enterprise mobility in action: case studies

Successful combined BYOD and corporate liable implementations

McCombs Enterprises

McCombs Enterprises is a Texas-based consortium, with different businesses in the areas of automotive, construction, development, broadcasting and sports. The automotive and construction businesses in particular wanted to enable push-to-talk services on 1,000+ corporate liable rugged devices for their mobile workforce to easily and directly communicate with each other regarding the status of tasks and activities, at the same time as rolling out and managing a variety of other apps. Previously, employees had needed to carry two devices around with them: one for push-to-talk, and one for everything else. McCombs had also noticed that employees were bringing and using their own devices even once they had been provided with one – or two – by the business, so they also wanted to manage this BYOD behaviour.

McCombs recognized the need to manage and secure the data and apps running on all these devices, whether corporate or personal owned, and enlisted the aid of mobile service provider AT&T. As well as providing an enhanced push-to-talk service that would work on the same devices as those used for every other app, AT&T bundled AirWatch MDM software to monitor and control devices all corporate liable and employee-owned devices, across the full range of operating systems in use.

The program has enabled technicians and managers to stop carrying multiple devices around with them, and collaborate on tasks much more efficiently. At the same time, the BYOD support has opened up mobile usage to a range of workers including those in sales teams who may not previously have been provided with any kind of mobile device at all. These personal devices can be locked or wiped just as easily as the corporate liable ones if they are lost or stolen, and there is an added benefit when staff leave the company. With a high turnover rate among sales staff in particular, McCombs can be sure that when they leave, they don't take sensitive business data and customer contacts with them. The corporate apps and data can be wiped over the air and the device effectively decommissioned – while still functional as a personal device of course – as soon as the employee goes.

Australian-based travel technology services and solutions firm

An Australian firm specializing in travel technology services and solutions has been aiming to mobilize its large team of field sales agents and client-facing technicians. The firm offers travel-related solutions in areas such as air, rail, car rental, hotel management, travel documentation, corporate booking tools, ticket automation, and as a technology provider itself it wanted to give its mobile workforce access to the latest apps and tools, as well as presenting a tech-savvy image to customers.

The firm wanted to roll out corporate-provided iPads, and also respond to employee demand to support BYOD for iOS devices, including iPhones and iPads. It is moving away from a COBO BlackBerry deployment, and chose a leading EMM vendor to manage and secure both the corporate liable and BYOD initiatives. Requirements of the program included: enabling easy administration without needing to expand the number of IT staff; role based configuration of policies and apps to differentiate between types of user and device (e.g. whether BYOD or corporate liable); providing a native user experience for the worker; roaming cost control for the firm's many international travellers; and remote data wipe for cases of device loss or theft.

Taking this approach has enabled the firm to expand the number of apps that employees can use, and the range of devices these apps can be accessed from. This has opened up new working styles and improved productivity, as well as improving the customer-facing image of the company. In addition, focusing on iOS as the sole supported mobile OS has reduced the complexity of managing the deployment, and the firm has allowed its employees to work in an unrestricted way – the only restrictions that it enforces on them are roaming control, PIN enforcement and blocking explicit content.

Appendix

Methodology

This paper draws on Ovum's extensive research into the enterprise mobility market, including surveys of employees, interviews and interactions with enterprise IT decision-makers, and in-depth analysis of supply-side vendor software and services.

Author

Richard Absalom, Principal Analyst, Enterprise Mobility and Productivity

richard.absalom@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer

CONTACT US

www.ovum.com
askananalyst@ovum.com

INTERNATIONAL OFFICES

Beijing
Dubai
Hong Kong
Hyderabad
Johannesburg
London
Melbourne
New York
San Francisco
Sao Paulo
Tokyo