Beyond BYOD: how businesses might COPE with mobility

Identifying the right mobility strategy for your organization

EXECUTIVE SUMMARY

Ovum view: BYOD is a behavior, not a strategy

There has been a lot of hype around the Bring Your Own Device (BYOD) trend over the last few years, and rightly so - Ovum research shows that around 57% of all employees worldwide are accessing corporate data in some form on a personal smartphone or tablet. But our definition of BYOD is that it is a behavior that is going on regardless, not a strategy that businesses must adopt. As we enter a mobile first environment and mobility becomes an increasingly important part of every IT department's service, getting device and application provisioning strategies right is vital. Understanding employee behavior and what is driving them to use their own devices at work is an important step in developing that policy, but a mobility policy does not just mean allowing and enabling employees to use their own devices for work.

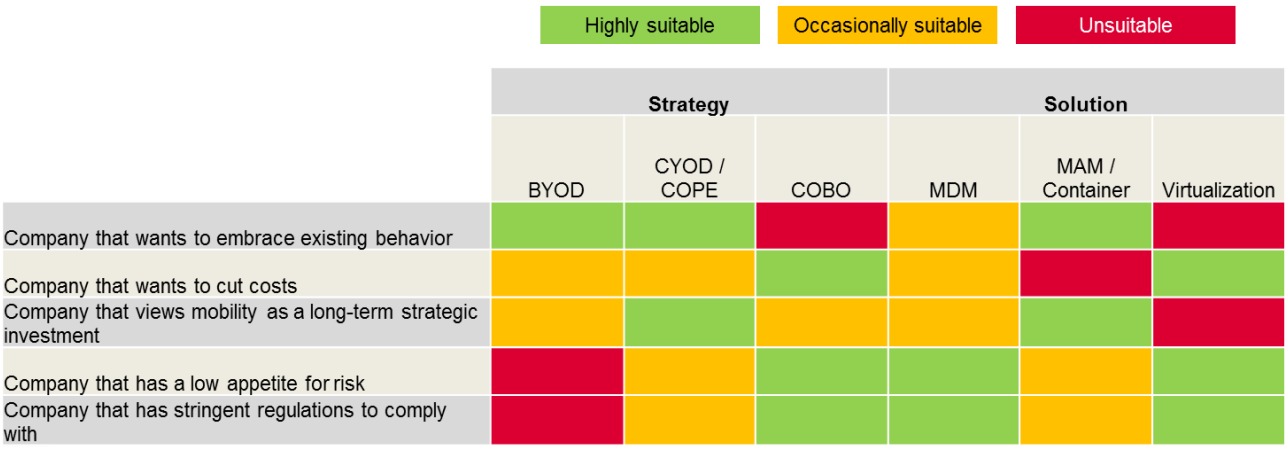
Regulatory and legal compliance issues, concerns over privacy, costs and the difficulties of managing such a fragmented array of devices and applications make fully supporting BYOD a real challenge for IT. For some, it will make sense to embrace BYOD, for others there are alternative options in corporate provisioning such as Choose Your Own Device (CYOD) and Corporate Owned Personally Enabled (COPE), which may deal with some of the behavioral drivers of BYOD and also make it easier for IT to manage the corporate mobile estate. Strategies such as CYOD and COPE demonstrate that the idea of providing a corporate-owned device to employees does not need to be as rigid as it used to be: Corporate Owned Business Only (COBO) is not the only option any more.

There is no one-size-fits-all solution for mobility

There is no silver bullet solution to this challenge, or a one-size-fits-all answer: every organization has different requirements. This paper aims to aid the process of working out which type of mobile strategy a business will choose to adopt. It examines the behavioral drivers of BYOD, and outlines the different strategic options around mobility that are open to the enterprise. Most importantly, it discusses which strategies and technical solutions are most applicable in different scenarios, taking into account an organization's attitude towards existing employee behavior and requirements, desire to cut costs, their view of mobility as a long term strategic investment, openness to risk, and any relevant regional or industry-specific regulations. Broad

recommendations on the suitability of different strategies and solutions are outlined in the following table:

Figure 1: Comparative suitability of different enterprise mobility strategies and solutions



Source: Ovum

Key messages

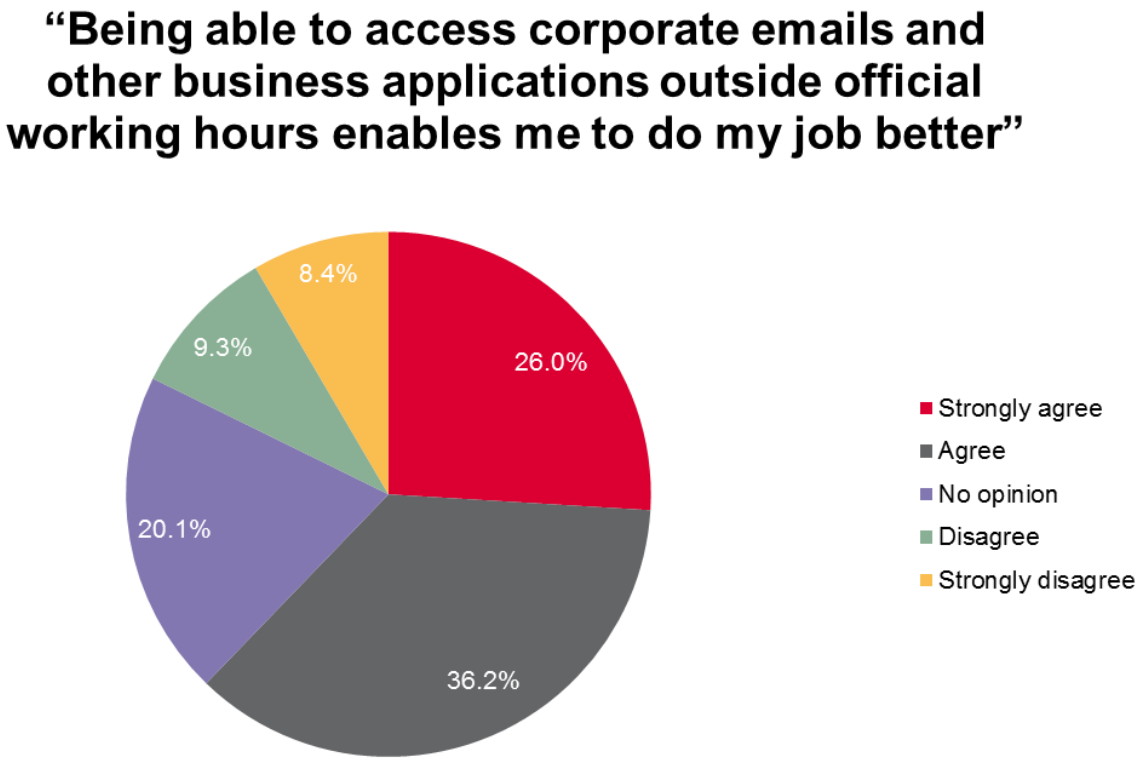
- Understanding the behavioral drivers of BYOD is the first step in establishing a mobility strategy that meets the requirements of employees and employer alike.
- There are several different strategic options to take: BYOD, CYOD, COPE, and COBO (Corporate Owned Business Only). Each has specific benefits and drawbacks, and will suit certain scenarios better than others.
- Once an organization understands the approach it wants to take, it needs to find a technical solution to match that strategy - not the other way round. There are various types of enterprise mobility management (EMM) solution on the market, each suited to certain scenarios. The most successful EMM solutions will be those that are able to support all scenarios, as businesses adopt a mix of strategies between different departments, vertical units and countries.

TABLE OF CONTENTS

UNDERSTANDING THE BEHAVIORAL DRIVERS OF BYOD

Employees want flexibility

Figure 2: Employees appreciate flexibility of access to key tasks out of normal office hours



Source: Ovum Multi-Market BYOD survey 2013, N = 4371

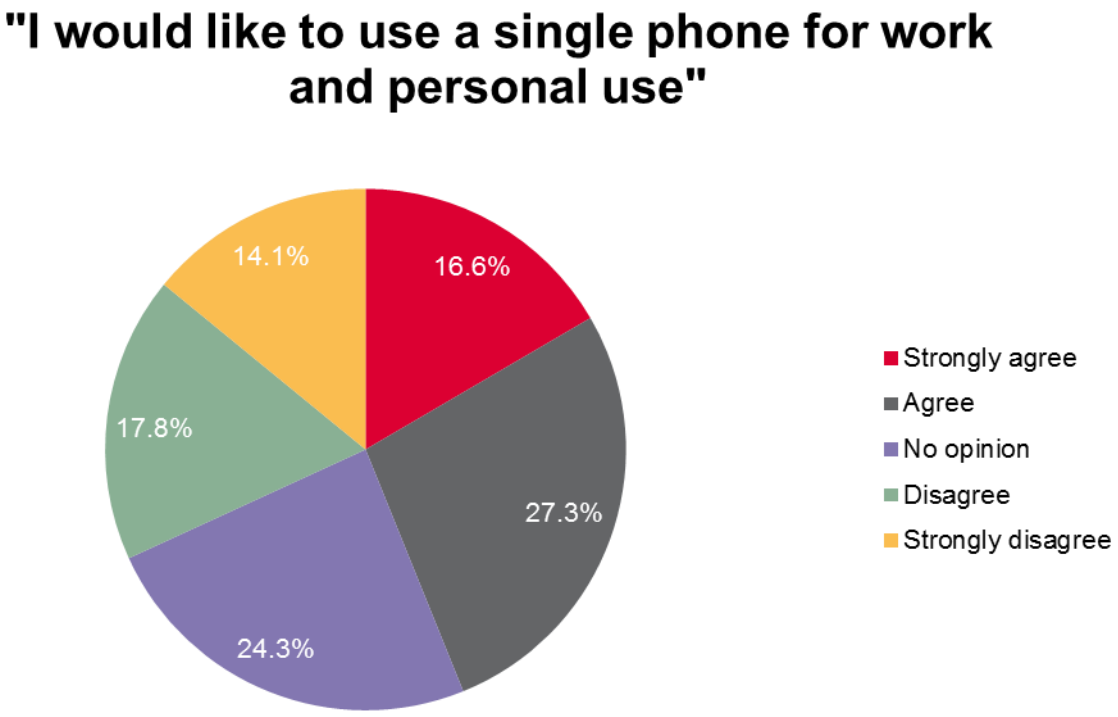
Ovum conducts an annual survey of full time employees across the globe, from all industries and in all types of job role, which allows us to identify trends in behavior and attitude towards the use of mobile devices and applications at work. Consumer innovation has propelled the mobility market in recent years, so this study helps to gauge trends such as the scale of BYOD, directly from those who are driving it. The latest research tells us that the majority of employees feel that access to corporate emails and content outside of normal office hours improves their ability to do their job well (see Figure 2). If employers do not provide staff with the tools to be able to do this, it naturally drives the use of personal devices and apps - workers will find their own ways to so their job better or make their life easier.

This wish to be flexible has been around for a long time, but the difference over the last five years has been the level of growth and innovation in the consumer mobile market, where the device renewal cycle is so fast that the enterprise cannot hope to keep up with it. This has raised employee expectations around what they can do with their devices, and made BYOD possible on a large scale - driven also by the factor that Apple and Google, the two primary drivers of growth in

the consumer space, have not up to this point prioritized enterprise features over consumer expectations.

A significant number of employees want to use a single device in all areas of their life

Figure 3: Desire to use a single device in just work and personal life is a driver of BYOD for many



Source: Ovum Multi-Market BYOD survey 2013, N = 4371

Initially, Ovum surmised that the preference to carry a single device around - rather than one for work and one for personal life - would be a primary driver of BYOD. In fact, as shown in Figure 3, this is not as big a factor as we might have imagined, but it is still an issue for quite a large percentage of employees - just under 50%.

This is something that will need addressing in every organization, but doesn't necessarily have to mean allowing BYOD. For an organization planning its mobility strategy, the key issue is to find out whether employees would mind if that single device they carried was a corporate-provided one. If not, having some kind of CYOD or COPE policy may be an ideal solution that addresses one of the key drivers of BYOD behavior as well as maintaining corporate management and control over the device.

THE DIFFERING STRATEGIC OPTIONS IN ENTERPRISE MOBILITY

Bring Your Own Device (BYOD)

While we have identified that BYOD is a behavior first and foremost, rather than just a strategy, many organizations are finding ways to encourage, embrace or formalize the behavior as part of their mobility strategy. Ovum believes that, broadly, there are three different "levels" of BYOD that organizations are choosing from:

- Unrestricted, supported BYOD: employees are allowed to use any personal device that they want for work and the company will aim to support it.
- Restricted, supported BYOD: employees are allowed to use a personal device for work as long as it is on a list of approved devices that the company will support.
- Unrestricted, unsupported BYOD: employees are allowed to use any personal device they want for work, but it is left unmanaged and unsupported by the company. This is not an option that Ovum recommends as it leaves data and devices essentially unmanaged, meaning risk in terms of data leakage and lack of protection against virus and malware - although, as outlined later in Figure 4, it is a tactic already in place at many organizations, perhaps as a temporary stop-gap measure.

The following outlines the pros and cons of a BYOD strategy in relation to key factors that may influence enterprise decision-makers.

Existing employee behavior, demands and requirements

As shown in Ovum's research, a BYOD strategy fits clearly with the existing behavior of many employees. More and more people own a smartphone and/or a tablet, and they are very likely to use those devices for work at least occasionally. The survey data tells us that almost 68% of smartphone-owning employees will use that device for work, as will almost 70% of tablet-owning employees. Having a BYOD strategy clearly taps into a behavior that is already evident on a widespread scale.

BYOD strategies also allow employees to have a choice and high level of flexibility over their preferred device to use at work. People choose particular devices for various reasons, but their choice is most often influenced by preference for a particular OS and the experience it offers, the range of apps on offer, or price and affordability. Mobile devices (and particularly smartphones) are now "digital limbs" to many of us, kept never more than an arm's reach away. They are used in all areas of our personal lives, and of course that generates demand to use these devices in our working lives as well. As the boundaries between work and personal life blur, this is a demand that a BYOD strategy easily fulfills.

Of course, a mobility strategy has an impact on all mobile users in a business - including that significant minority who don't want to bring their own. A BYOD strategy would not be favorable to those employees who feel like it is the responsibility of their employer to give them the tools they need to do their job. Therefore, understanding the prevailing attitude with an organization -

whether people already use their own devices or would like to be able to or not - is of vital importance in understanding whether the strategy is a correct fit.

Desire to cut costs

Embracing BYOD can mean savings around hardware as the cost of the fast renewal cycle in the mobile space is passed on to employees. But organizations should be aware of false economies: corporate owned devices provided with a contract are often heavily subsidized anyway, and the services likely to be required to support personally owned devices also come at a cost. Subsidizing or expensing personal call plans for work usage is also far more expensive than having a corporate-negotiated tariff, with studies from telecoms expense management (TEM) vendors showing that exactly the same activities can cost up to 5x more on a personal plan than on a business plan.

The view of mobility as a long term strategic investment

A BYOD strategy can be viewed in two ways: it is either a stop-gap that lets employees make use of the powerful devices they own while the business catches up to the possibilities they offer; or a view that innovation in the consumer tech space has outstripped that in the enterprise and there is a need for IT to open up and embrace change just as employees' habits and expectations change. Rather than trying to keep up with provisioning the latest devices, a long-term BYOD strategy recognizes that the best way to do that is to let employees have the freedom to use the devices of their choice.

There is a sense at the moment that in many businesses BYOD is happening despite enterprise IT, not because of it. Mobile strategies are largely a reaction to a particular behavior rather than a push to proactively drive mobile usage and productivity, so it will be interesting over the next 18 months to gauge the extent to which the enterprise moves away from BYOD and adopts such strategies as CYOD or COPE, as they get to grips with the demands of employees and think about how mobility can benefit them in the long term.

Risk profile

Although it can be managed and secured with various enterprise mobility management (EMM) solutions (examined later in this paper), BYOD is not a strategy highly favored by organizations with a low appetite or threshold for risk. Managing a BYOD environment, by definition, entails managing a heterogeneous environment with multiple platforms and device types. And for certain organizations with a high focus on data security such as those in the public sector, healthcare or banking, that introduction of so many variables is a scenario that they don't want to negotiate - there are too many points at which data can be vulnerable if not managed meticulously well. For these types of organizations, a corporate-owned strategy of some kind is often preferable.

Regional and vertical legislation

As in any situation, organizations need to be well aware of the legislation and regulations that have an impact on their mobility strategy. For instance, BYOD is simply against the law in some verticals - in the US, the Health Insurance Portability and Accountability Act (HIPAA) doesn't allow for patient data to be accessed on personally owned devices. In highly regulated industries where the ability to monitor and log all device activity is required, a restricted BYOD strategy may still be

possible (the devices allowed would need to support the required monitoring and security features) - but businesses then need to be very careful then about employees' data privacy. If their employer deploys MDM software on personal devices that is able to monitor, lock and wipe data, employees need to be aware of, and provide consent for, that software to be deployed. If this consent is not given and personal data is accessed or even wiped, the employer is breaching individual data privacy legislation in practically every country, and could face a lawsuit from their own employees.

From this point of view, BYOD is not always the easiest or most suitable strategy to adopt. Indeed, for some organizations (particularly in the government and defense sectors), regulations mean that it is impossible to legally operate a BYOD strategy. For example, the US Department of Defense (DoD) requires mobile device vendors to hold Full Operational Capability (FOC) certification on devices used to access DoD systems and data - and only BlackBerry currently holds that certification. In industry sectors where it may be possible but difficult to implement BYOD, it is also worth looking at corporate-owned strategies that embrace some of the same drivers around employee behavior and expectations.

Choose Your Own Device (CYOD) and Corporate Owned Personally Enabled (COPE)

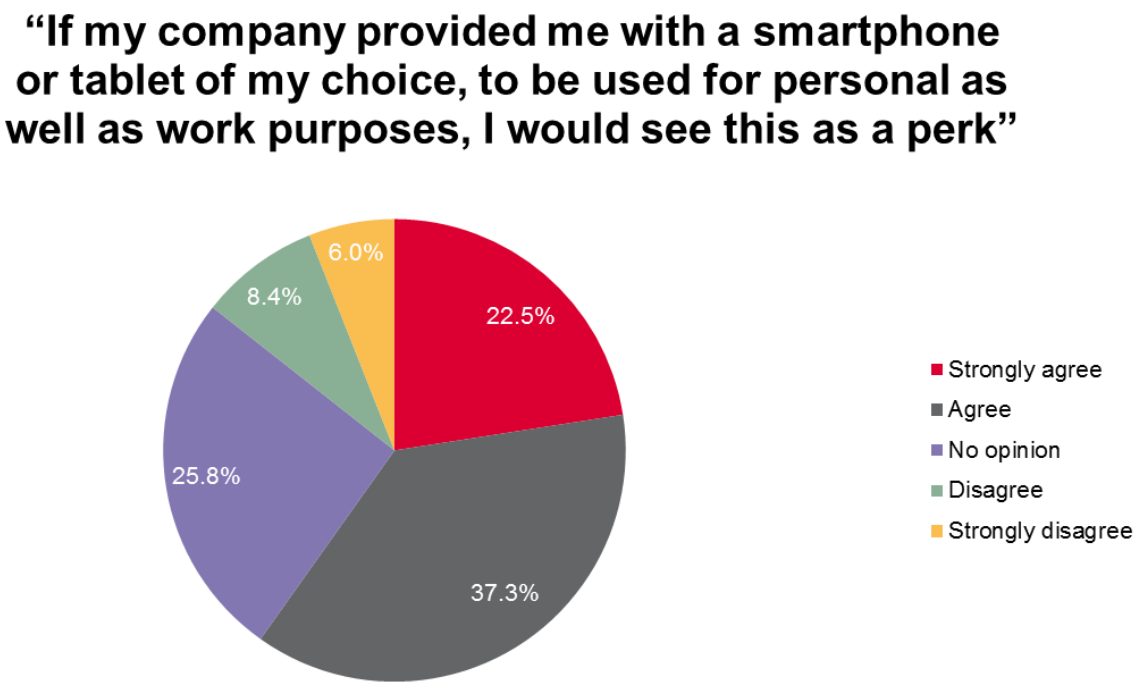
Choose Your Own Device (CYOD) refers to a strategy where organizations give their employers a choice of devices to use at work. It is often used alongside a Corporate Owned Personally Enabled (COPE) model, where the employee is allowed to use the device for personal activities even though the device remains the property of the business. In some ways, CYOD and COPE strategies are a happy medium for enterprise IT, between the risks and uncertainty of BYOD and inflexibility of no choice corporate provisioning, or Corporate Owned Business Only (COBO) deployments. CYOD and COPE strategies demonstrate that corporate provisioning does not have to be as rigid a process as it once was - it is not just about giving someone a device to use and expecting them to be happy with it.

The following outlines the pros and cons of a CYOD / COPE strategy in relation to key factors that may influence enterprise decision-makers.

Existing employee behavior, demands and requirements

Ovum's survey data shows that the majority of employees would find a mixed COPE / CYOD strategy appealing. See Figure 4: almost 60% either agree or strongly agree that being given a device to use for personal as well as work purposes would be a perk, while only 14.4% disagree with that opinion. Such a strategy is likely to prove popular, therefore, and it also clearly addresses some of the drivers of BYOD behavior.

Figure 4: Employee attitudes to COPE are largely favorable



Source: Ovum Multi-Market BYOD survey 2013, N = 4371

A CYOD strategy meets the demand from employees to choose the device they want to use at work, as long as the choice of devices on offer is broad enough. And if offered as part of a COPE strategy as well, it would meet the demand from the 44% of employees to use a single device for work and personal activity. In this way, it addresses two of the key drivers of BYOD behavior, but provides the benefits to IT of having a corporate provided device.

Desire to cut costs

If an organization wants to provide a choice of high-end devices, CYOD is likely to lead to higher costs than in a model where employees have no choice over the device they are given to use. Apple in particular is notorious for not offering bulk discounts on its products even for orders numbering in the thousands, so businesses will be faced with paying retail prices. If offering a choice of low-end devices, there may be some cost savings, but this is less likely to meet demand for the latest and greatest gadgets - and in turn may drive some users back to their BYOD ways.

On the other hand, there is the view that corporate provisioned devices save on the potential costs of data lost through usage on unsecured personal devices. These savings are impossible to gauge exactly. A 2013 study by security firm Symantec and Ponemon Institute found that the average cost of a single data breach was $136 per record, with the average number of breeched records exceeding 23,000. In the US, where the average cost per record is $199, the highest total cost for a data breech was $5.4 million. However, you can't prove what a data loss incident that hasn't

happened will cost a particular business in terms of reputation damage and direct revenue loss or regulatory fine. But for organizations with a strong security focus, this is another argument to support deployment of corporate owned devices.

The view of mobility as a long term strategic investment

Choosing a CYOD / COPE strategy is indicative that a business believes in mobility as a long term strategic investment: it is actively looking to put these devices in the hands of employees and give them tools that they are comfortable working with, making them more efficient and productive. And if the organization is able to keep up with the renewal cycle of these smart devices, it will be able to consistently leverage their ever-growing capabilities and processing power to enhance the range of apps and services that employees can make use of.

Risk profile

For organizations that have a conservative approach to risk, CYOD and COPE are good options as long as the required security features are possible to implement across every device that they offer users. It allows flexibility around device choice, but also for the business to maintain full control and management of that device.

Regional and vertical legislation

Corporate-owned devices are less likely to fall foul of privacy and data security regulations: the organization has the freedom to install security and management features that meet the requirements specified by their regulator. Care still needs to be taken over access to personal apps and data even if on a corporate device, and organizations need to be aware of privacy legislation in different countries. For example in Germany, personal-related mail and data may still be subject to personal privacy legislation even if accessed through a corporate service and on a personal device.

Corporate Owned Business Only (COBO)

Prior to the onset of consumerization and BYOD, Corporate Owned Business Only (COBO) strategies were the primary model around which organizations supplied key employees with mobile working capabilities: users are given a device to use (often there is no choice over which device to use, but that does not necessarily have to be the case), and restricted to using it for business purposes only. This model has become largely outdated among organizations that do not have high security requirements as high connectivity and cloud applications make it easy for employees to access multiple types of content from the same device, including of course consumer-related services such as email and social networking. It does however still have a place for certain types of organization and user.

The following outlines the pros and cons of a COBO strategy in relation to key factors that may influence enterprise decision-makers.

Existing employee behavior, demands and requirements

The COBO model does not meet employee demand for flexibility over the device they use, or the desire to use a single device for both work and personal activity. However, there is still a segment

of users - especially in developed markets - who have become accustomed to a certain way of working and want their employer to provide them with all the tools they need, and keep their work and personal lives completely separate. A COBO strategy would still fit this segment of users perfectly well.

Desire to cut costs

This strategy is potentially the cheapest of all the options, as the hardware is likely to come subsidized with a corporate call plan, and expenses can be kept in check. As most organizations are likely to be coming from the position of having a COBO strategy, however, this is more a case of maintaining spending levels rather than significantly raising or lowering them. It should also be noted that a BYOD strategy, for instance, would allow for more of the workforce to be mobilized without the business needing to fork out for their devices. To extend the number of mobilized workers through a COBO model would entail increased costs as more devices and call plans are provisioned.

The view of mobility as a long term strategic investment

Unless devices are constantly updated, which is unlikely given the fast launch cycle, COBO does not take into account the fast changing nature of mobility, and risks leaving users behind in terms of what they can and cannot do on a device - it is hard to keep up with all the new feature additions. Enabling mobility as a strategic investment is about giving users flexibility - and COBO is the least effective way of doing that out of all the options covered in this paper.

Risk profile

In terms of data security and management, COBO should be the least risky model. Organizations can install whatever solutions they deem relevant on the devices and keep complete control over what can and can't be accessed on them - they can lock devices down as much as required. This means that using COBO devices can be the safest option, but the risk is in providing a poor user experience and restricting access to desired applications, driving employees to find ways around the system and finding other ways to do their job i.e. turning them back to BYOD.

To negate the risk around user experience, having an end-to-end EMM solution for COBO - e.g. one that supplies the device, secure infrastructure and the management software - would enable a consistent experience and also allow for newly released devices to be supported easily. BlackBerry is the originator and most prominent vendor offering this all-inclusive hardware and software package for COBO deployments, and remains the leader in terms of end-to-end device security and management - although it looks like Samsung is targeting the space with its Knox devices, and it is also potentially an area of interest for Microsoft and Widows Phone.

Regional and vertical legislation

As with any corporate-provided scheme, having a COBO strategy makes it easier to comply with regulations and legislation. In this case there is far less to worry about around employee privacy: stating that a device is for business use only means that employees using them for personal communications can have no complaints, for example, when the device is remotely locked or wiped.

APPLYING SOLUTIONS: MATCHING TECHNOLOGY TO STRATEGY

Identify the required strategy first - then look for a solution

Once the right strategy that fits the particular needs of the business has been found, it is important to find the right management solution that fits that strategy. Finding a solution first and trying to tailor a strategy to fit those capabilities would be a severe case of letting the tail wag the dog.

There are several approaches that various software vendors are taking to managing mobility in the enterprise, and here we examine how suitable mobile device management (MDM), mobile application management (MAM) and containerization, and virtualization are to the different types of strategies discussed above. These different solution approaches all fall under the umbrella term of enterprise mobility management (EMM), and we often see them deployed in conjunction with each other - emphasizing that some are more suited to certain scenarios within a business than others.

Mobile Device Management (MDM)

MDM solutions provide device-level security and management through a client installed on a smartphone or tablet (the majority of devices do not come with native control pre-installed). Key features include: over-the-air device enrolment (authentication and policy configuration), enabling user and group-specific policies to be set; password / PIN policy enforcement; full, partial or selective remote data wipe; GPS tracking, geofencing (i.e. enabling / disabling certain applications or components depending on location); device activity logging for full audit trail; real time activity reporting and alerts; and secure email gateway (i.e. controlling, monitoring, blocking access to email based on user / device / device type).

Suitability to BYOD

MDM solutions can generally be applied across all mobile operating systems, so it can work in a BYOD scenario and we have seen many organizations implement it. However, MDM entails the full control of a device and this is unlikely to go down well with employees - they don't want their employer to see what they are doing in their personal time. Ovum has seen examples of employees refusing to sign up to a BYOD policy, or reacting strongly against it, when they realize the full extent of what a MDM client can do with their device.

Suitability to CYOD / COPE

As with a BYOD strategy, MDM covers all the requirements in terms of device and OS coverage, and provides numerous safety and management features. And on a corporate-owned device, there can be less room for complaints from employees about being able to do things like remotely lock a device or wipe all data from it - although in an ideal scenario, work and personal data should still be kept separate in a CYOD or COPE strategy.

Suitability to COBO

MDM is highly suited to a COBO strategy, where IT is aiming to manage and secure all apps and data on a device, and there is no need to separate work and personal data.

Mobile Application Management (MAM) and Containerization

MAM solutions provide app-level security and management, enabling businesses to deploy and manage apps across registered mobile devices. Features include push services (i.e. automatically pushing apps to devices, over the air); app discovery and delivery through an enterprise app store or app catalog; provision of bespoke, custom developed apps and publicly available, third party apps; and app usage analytics.

MAM solutions are often deployed in conjunction with or as part of a container: a secure area on a device that keeps business apps and data separate from everything else on the device and allows enterprise IT to manage only what is in the container, leaving the rest of the device alone. This container might look like an application, or it could be an entirely different persona on the same device (e.g. BlackBerry Balance or Samsung Knox).

Suitability to BYOD

MAM and containerization provide a "lighter touch" method of management than MDM, and focusing on managing the apps rather than the whole device makes this an attractive proposition for a BYOD scenario - it is easy to separate work and personal data, apps and activities, which is ideally what you are looking for when employees are using their own devices. User experience is important though, and some may not like the idea of having to sign into a separate container to access their work apps, or having all their contacts separated down work and personal lines - for some, it is much harder to keep work and personal life separate and indeed they may like those lines to be blurred. Trialing MAM solutions and gauging employee attitudes and reactions to them is important before going ahead with a large-scale implementation.

Suitability to CYOD / COPE

MAM, on its own, may not offer quite the level of security as MDM, in that usage of apps outside the container or out of the sphere of IT control cannot be monitored, but is often deployed in conjunction with MDM. In a CYOD or COPE strategy, it enables employees to access the productivity apps that they need, and also for work and personal apps to be secured and managed separately. So it is suitable, and doubly so if it meets an organization's security requirements either on its own or in tandem with MDM.

Suitability to COBO

There is not the same demand in a COBO strategy to keep work and personal activity separate, so a container may not be necessary, but it's still important to offer employees they apps they need. So MAM comes into play here from a productivity point of view, if not from a pure security standpoint.

Virtualization

Virtualization entails deploying a virtual private network (VPN) to a device, enabling the user to access a virtual desktop environment on whatever device they happen to be using - as long as they have a connection. This approach is highly secure, ensuring that no data is ever stored locally to a device, but it has a significant downside in terms of user experience.

Suitability to BYOD

Providing a virtualized environment is a very safe way of doing things, but comes up against a couple of problems in a BYOD scenario: firstly, it requires a constant connection; secondly, it has a massive impact on the user experience. People choose certain devices because they like the OS and the interface, and virtualization removes that experience with something not specifically designed for a mobile device. It is difficult to recommend virtualization as a suitable approach to managing a BYOD strategy.

Suitability to CYOD / COPE

Virtualization is not recommended in a CYOD or COPE scenario for the same reasons as in BYOD - it disrupts the user experience and takes away the point of offering employees a choice over which device they use.

Suitability to COBO

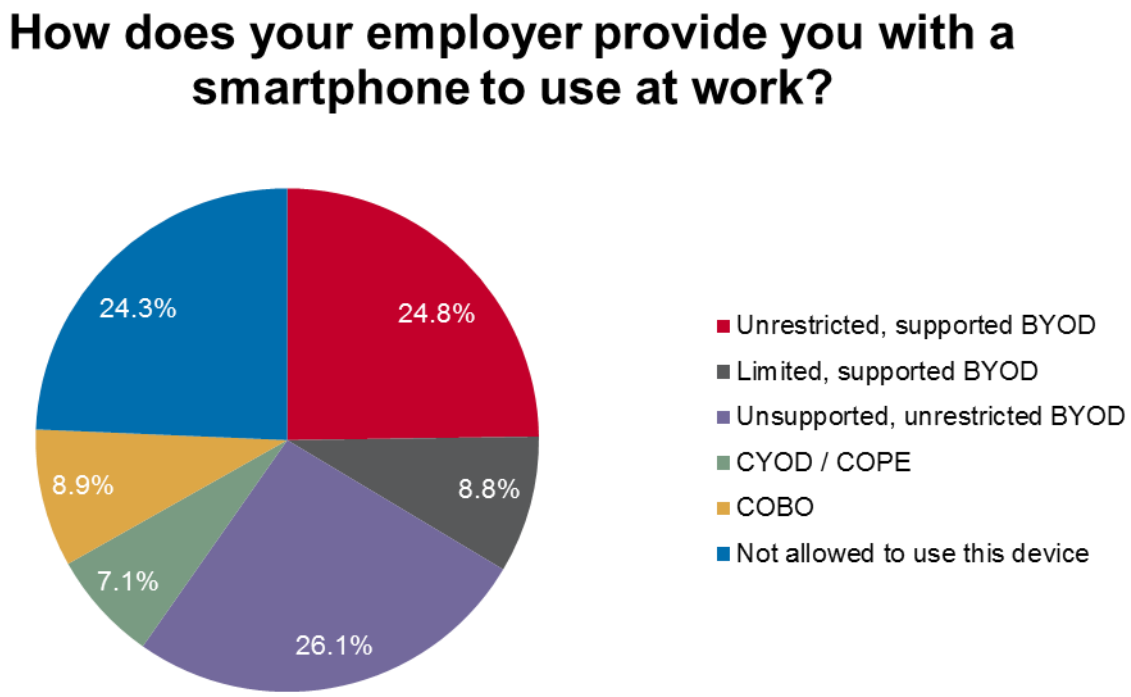
The issues over user experience still remain in a COBO strategy, but a virtualized environment does provide a highly secure way of working on a mobile device. It allows for access to sensitive corporate data from anywhere a connection is available, and can prevent any of that data from ever being stored locally on the device. In a scenario where there is low appetite for risk, or where data security is of absolutely paramount importance, virtualization has a place - and in that kind of organization, COBO is more likely to be in place anyway.

CONCLUSION

It is clear that when it comes to planning and implementing a mobility strategy, there is no one size fits all policy that suits all organizations - or even all roles within a particular organization. Ovum thinks that we will see the majority of firms adopt a mix of BYOD, CYOD, COPE and COBO strategies, applying different rules to different teams and employees depending on their particular requirements, security profile, risk profile and the kind of apps and the type of data that they need access to. Having an EMM solution capable of supporting all scenarios simultaneously would therefore be advantageous to organizations implementing mixed corporate and personally owned device deployments.

The survey data in Figure 4 shows the mix of strategies that we see around smartphones in particular at the moment: BYOD in its various forms is widespread, while at the other end of the scale almost a quarter of employees are still discouraged or not allowed to use smartphones.

Figure 4: Current spread of enterprise mobile provisioning strategies



Source: Ovum Multi-Market BYOD survey 2013, N = 4371

BYOD strategies continue to gain popularity and are becoming formalized on a widespread basis - we expect that the proportion of unmanaged (e.g. unsupported, unrestricted) BYOD will shrink, as businesses either choose to embrace BYOD or adopt CYOD or COPE. These alternative corporate-provisioned strategies will take off among organizations that appreciate the flexibility but don't want the risks of BYOD.

Ovum views COBO strategies to be suitably applicable or advisable in highly regulated environments and verticals, where there is a lot of sensitive data in use and a low appetite for risk. In these scenarios, employees should also be well aware of their responsibilities and reasons for not using devices and applications built primarily with consumers in mind in the working environment.

In choosing a mobility strategy, every organization needs to make its own decision based on the combination of factors discussed in this paper: the regulatory and legal constraints it faces, the attitude it has towards risk, existing behavior and demand from its employees, and a consideration of the specific business processes that can benefit from being mobilized. There is, simply, no single right or wrong way of doing things - but there are certain strategies and solutions that may be more of a suitable fit in different scenarios.

APPENDIX

Author

Richard Absalom, Senior Analyst, Enterprise Mobility

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.

Disclaimer

The facts of this report are believed to be correct at the time of publication but cannot be guaranteed. Please note that the findings, conclusions, and recommendations that Ovum delivers will be based on information gathered in good faith from both primary and secondary sources, whose accuracy we are not always in a position to guarantee. As such Ovum can accept no liability whatever for actions taken based on any information that may subsequently prove to be incorrect.