>>

WHITEPAPER

Enterprise mobility trends 2015 and beyond

How to best manage mobile in the workplace and deal with challenges from current and emerging technologies

FEBRUARY 2015

V3resources

Contents

V3 provides technology professionals with 24/7 news and analysis on the happenings of the IT industry. V3 serves an audience of IT buyers and business decision-makers with up-to-the-minute news, reviews and analysis written by a team of expert IT journalists in the UK and Silicon Valley. V3 delivers real-time IT news, features and analysis alongside product reviews, software downloads, video demos, blogs, white papers and IT jobs to a broad audience of IT professionals and enthusiasts. V3 is published in the UK by Incisive Media, the trading name of Incisive Financial Publishing Limited.

Introduction

One of the biggest trends arising from the push to mobile is the expectation among employees to be able to use a smartphone, tablet or laptop for work purposes and at a time and location that suits their lifestyle. Workers are no longer content to sit at the same desk day in day out to get their jobs done; they instead expect to be able to work remotely, or from home, and use a device that allows them to carry out tasks wherever and whenever suits them.

This shift is putting pressure on firms to manage the plethora of new personal devices that have infiltrated their way into the workplace, but also offers benefits for businesses that are able properly to support mobile working.

This paper aims to uncover business attitudes towards enterprise mobility, including current approaches, and how these are likely to shift in the future as new devices and business models evolve. *V3* surveyed IT professionals on the devices and mobile platforms with the widest support within their organisations, the key benefits of and challenges arising from enterprise mobility, and whether tools or processes are in place to manage these devices.

Mobility benefits

The demand for a change in working patterns that has arisen from the rise of the mobile is reflected in our survey results. Support for flexible and remote working is the number one advantage for businesses supporting mobile use at work, chosen by 86 percent of respondents.

Figure 1: What are the biggest benefits for companies supporting mobile use at work?

|	
Allows flexible, remote working	**86%**
Increased staff productivity	**64%**
Cost savings	**39%**
Access to cloud services	**30%**
Staff manage their own devices so reduced IT admin	**29%**
Attracting staff to our company	**13%**

And this shift has benefits for employers as well as their staff. Almost a third of respondents (64 percent) cited increased staff productivity as a core benefit of the shift to mobile, indicating a high level of awareness that businesses can get more out of their workforce by making the transition to enterprise mobility.

The financial incentive was also important for many respondents, with 39 percent noting cost savings as a key benefit of mobile working, while allowing access to cloud services was important to 30 percent of organisations.

MaaS360®
by Fiberlink, an IBM company

Approaches to mobile management

Understandably, businesses have responded to the many benefits on offer by moving to support mobile in the workplace. It is encouraging to see that 28 percent of firms support a variety of mobile use cases, including bring your own device (BYOD), allowing staff to connect their own smartphone or tablet to work systems; choose your own device (CYOD), where staff are supplied with mobile devices from a pre-approved list; and BYOC, where employees can use their own computer or laptop for work.

Figure 2: Which approach is your firm taking to managing employees' mobile devices?

Staff are not allowed to use mobiles for work purposes (13%)

BYOD - we let staff connect their own phone or tablet to work systems (25%)

A mix of BYOD/CYOD/ BYOC (28%)

CYOD - staff are supplied with mobile devices from a pre-approved list (26%)

BYOC - employees can use their own computer or laptop for work (8%)
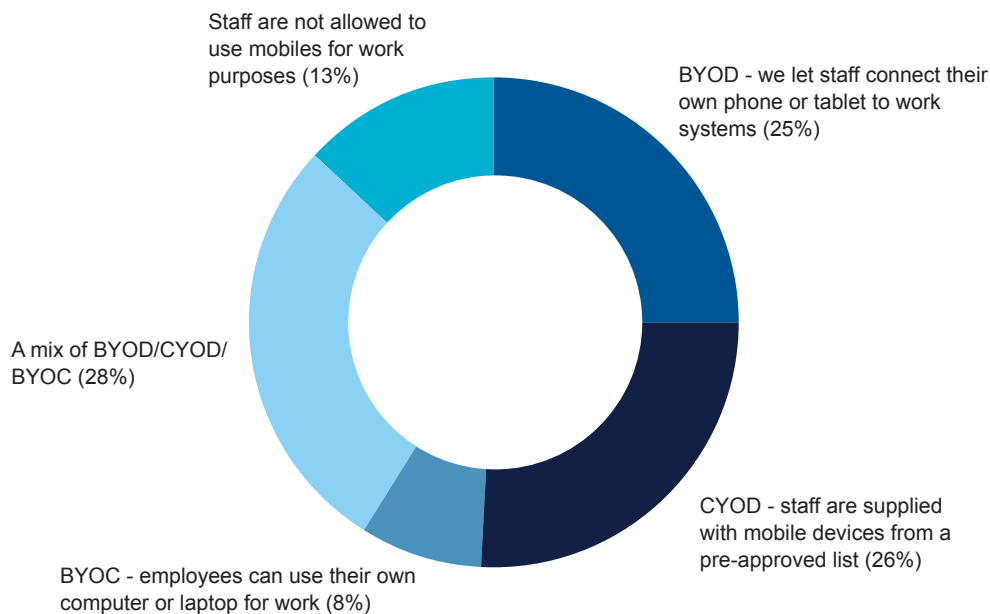
A further 26 percent have adopted CYOD as their primary approach to mobile in the workplace, while another quarter of businesses are supporting BYOD in the main. Only eight percent of respondents said that BYOC is their top choice for enabling mobile at work.
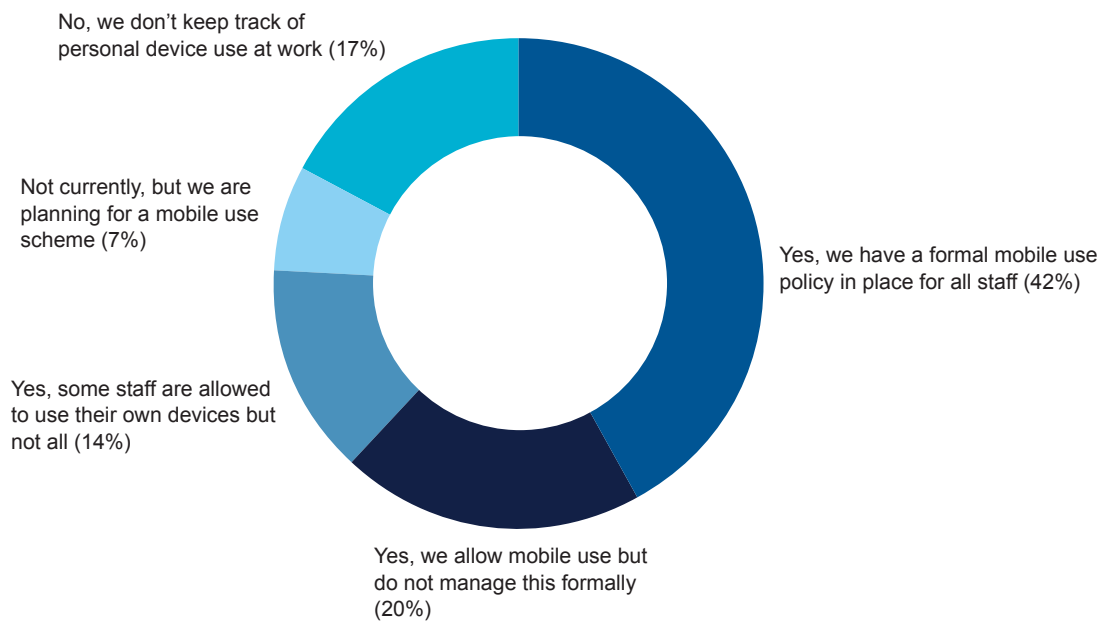
Whichever approach firms are taking to mobiles in the workplace, sandboxing is advised, allowing IT teams to partition off an area of the device that has additional protection measures. This allows IT to have more control to enforce certain policies and ensure that sensitive corporate data is protected.

It is worrying to see that 13 percent of organisations are still not allowing staff to use mobile devices at work. Of course, there are certain industries such as the financial, government or military sectors where mobile use would need to be highly restricted; but not allowing staff to use tablets or smartphones at all could result in these organisations falling behind their competitors which are finding ways to support mobile devices in a manner appropriate to their policies and regulations.

Despite the high proportion of businesses that allow staff to use smartphones, tablets or laptops for work, the majority have not adopted any formal processes to manage these devices.

While 42 percent have a formal mobile use policy in place for all staff, a fifth of respondents said their firm lets staff use mobiles at work but does not manage the devices with any set processes. A further seven percent of firms are planning a mobile use policy but have nothing in place at present.

Figure 3: Does your organisation have a mobile device strategy?

No, we don't keep track of personal device use at work (17%)

Not currently, but we are planning for a mobile use scheme (7%)

Yes, we have a formal mobile use policy in place for all staff (42%)

Yes, some staff are allowed to use their own devices but not all (14%)

Yes, we allow mobile use but do not manage this formally (20%)

More worrying is the 17 percent of organisations that do not even keep track of whether staff are using personal devices for work purposes, meaning they have no insight into or control over the corporate apps or data being accessed.

Larger organisations tend to be further ahead than their smaller counterparts at having formal mobile use policies in place, although small and medium-sized businesses are catching up. For firms starting the journey to mobile management, it is advisable to begin with a policy, covering factors like which data needs to be secured, which employees need access, and any regulatory requirements, and then find tools and technologies to help manage and enforce the rules.

Devices and operating systems

When it comes to the devices organisations are most comfortable supporting for use in the business, laptops and smartphones are almost tied at the top of the list, with 81 percent and 80 percent of firms respectively supporting these two mobile device types.

Figure 4: Which of these devices is supported by your organisation?
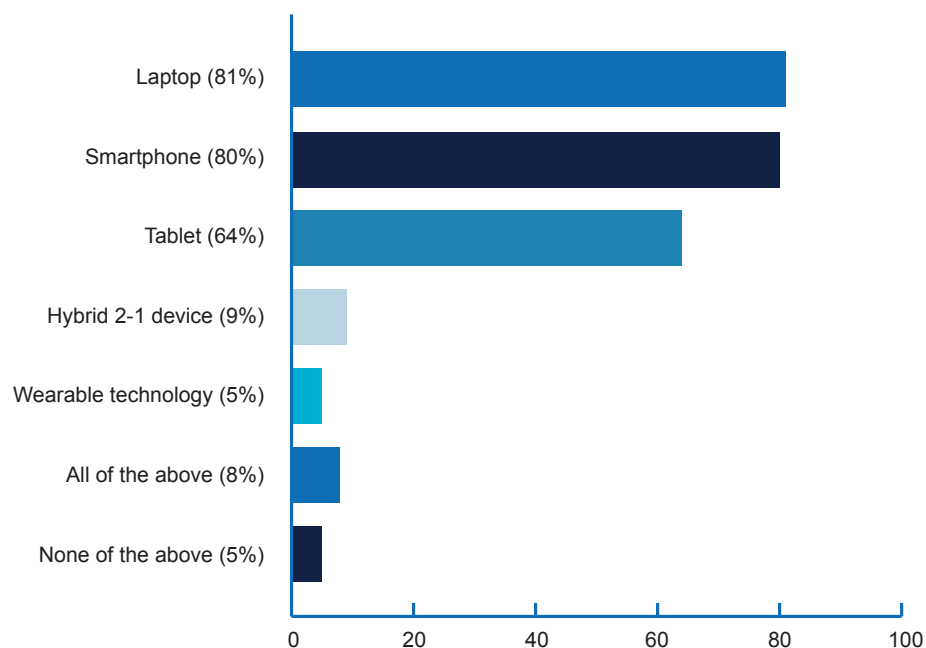
Tablets are supported in almost two-thirds of businesses (64 percent), and after this there is a huge chasm in support for other types of mobile device. Only nine percent of respondents said their organisation currently supports hybrid two-in-one devices, the most common being a tablet/laptop combination, while five percent offer support for wearable technology such as smartwatches or smart glasses.

Fewer than one in 10 respondents said that their business supports all of these different mobile devices, while five percent said that none on the list was enabled for their business.

While laptops, smartphones and tablets are the current leaders in this field, and are now widely supported and used for work purposes, it is likely that, beyond 2015, wearables and two-in-ones will move onto the radar of more organisations. This shift will come from employees opting to use devices like the Apple Watch or Google Glass, and expecting to access their work applications on them, and from businesses identifying vertical specific use cases that could have benefits for their sector, for example field workers or healthcare professionals.

Of the four main mobile operating systems – iOS, Android, BlackBerry and Windows Phone – only 13 percent of organisations offer support for all four within the business.

Unsurprisingly, iOS has the highest amount of support, at 57 percent. This is likely to be down to two factors: first, the preference for Apple iPhones and iPads among staff, but also as the Apple platform is widely seen as offering the best inbuilt security.

Figure 5: Which of these mobile operating systems is supported in your organisation?
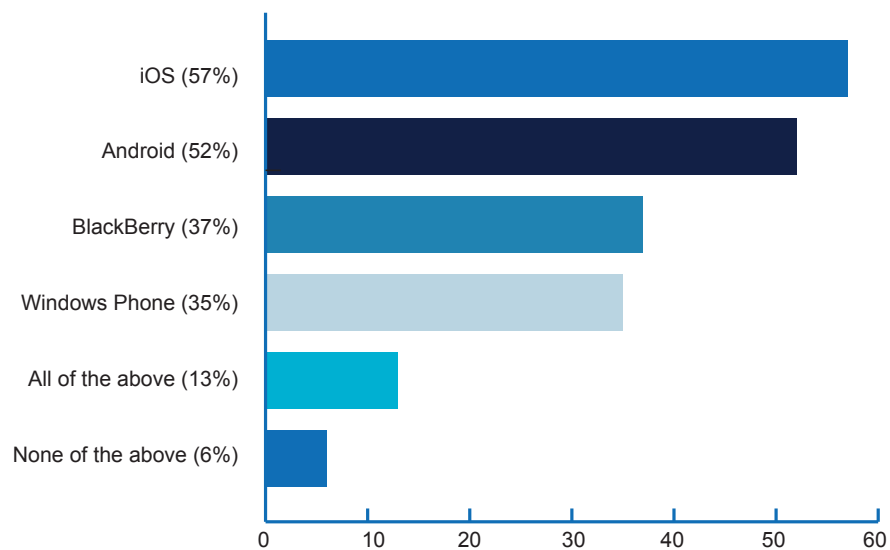
However, Android is hot on the heels of iOS, with 52 percent of respondents saying that the Google mobile operating system is supported by their business. BlackBerry and Windows Phone are neck and neck with support at 37 percent and 35 percent of organisations respectively. This is positive news for Microsoft, whose mobile platform is a newer entrant to the pack, and yet more evidence of the continuing decline of the BlackBerry, once the primary enterprise mobility tool.

However, IT professionals do not necessarily agree with these rankings. While iOS was chosen as the most suitable operating system for use in the enterprise by 26 percent of respondents, making it the top choice for IT staff, Android came third in this list with a fifth of the vote. Windows Phone garnered slightly higher support among IT professionals, at 22 percent, no doubt prompted by the continued prevalence of Windows machines in the enterprise, meaning integration benefits between desktop and mobile.

Figure 6: Which of these mobile operating systems is best suited for use in the enterprise?
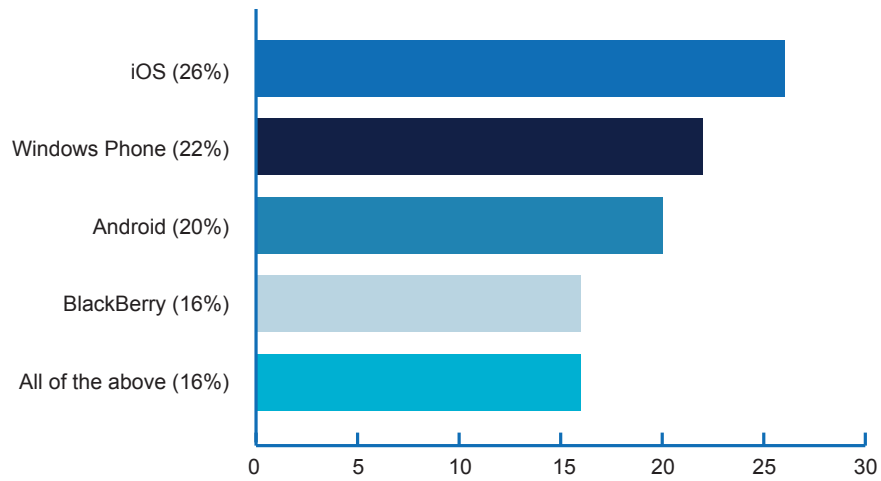
BlackBerry received only 16 percent of the vote, a sharp decline on what it is likely to have scored if this same survey had been run five years ago.

Risks and challenges

With the various mobile devices and platforms already available and being used for work purposes, coupled with emerging technologies like wearables and hybrid two-in-ones, it is unsurprising that almost half of respondents cited the pressure on the IT department to offer mobile support as a current challenge.

However, the biggest risk from enterprise mobility that IT professionals are concerned about is the security issues that could arise from the loss of devices.

Figure 7: What are the biggest risks of the shift to enterprise mobility?

Device loss leading to security issues	61%
Lack of control over corporate data access	49%
Requirement for IT to help users with numerous devices and platforms	48%
Staff accessing consumer services for work purposes	28%
Cost of supporting mobile devices	25%
Requirement for IT to create apps for multiple platforms	20%
Lack of transparency into use of services	19%

MaaS360®
by Fiberlink, an IBM company

This was closely followed by the lack of control firms have over access to corporate data now that so many employees use their mobiles for work purposes.

Much lower down the list of priorities for IT professionals tasked with supporting mobiles in the workplace were staff using consumer services, the cost of support and the need to create apps for different platforms.

Although security issues and data protection are high up on the priority list for IT professionals when it comes to their mobile strategies, this is not always reflected in practice. Despite a range of security measures being available to ensure that mobile devices are protected when used for work, whether these are company or staff-owned, 13 percent of businesses are not using any of these tools.

The most popular method for securing smartphones and tablets used at work is to enforce passwords for device and app access, but this is still used by only 58 percent of firms.

Figure 8: Which security measures are in place for work use of tablets and smartphones at your company?

Enforced passwords on mobile devices and apps	58%
VPN for network access	50%
Antivirus software installations	49%
Endpoint security on devices	41%
Remote file-wiping tools	33%
Download approval process for apps	24%
None of the above	13%

Half of respondents said that they require staff to go through a VPN for access to the corporate network, while around the same number said that they have antivirus running on mobile devices.
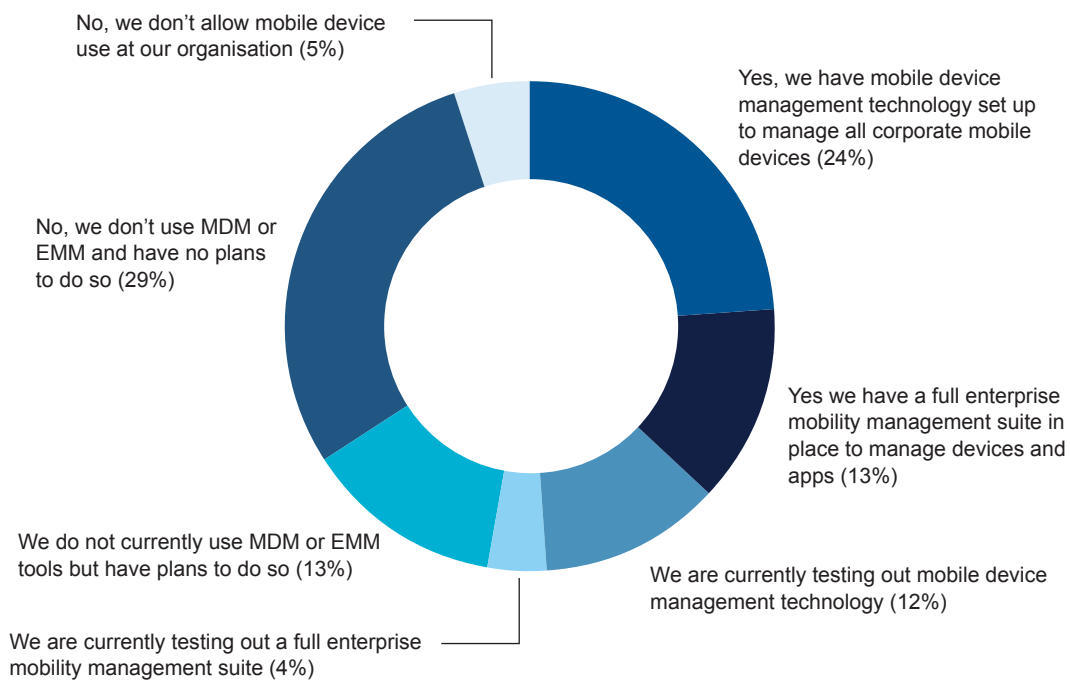
Few businesses are currently exerting much control over which apps their staff are downloading on work mobile devices, with less than a quarter requiring a download approval process.

Mobile management tools

Despite the lack of security tools in place to protect work mobile devices, it is encouraging to see that two-thirds of firms are currently using or testing technologies to manage their mobile estate, or have plans to do so.

Almost a quarter of businesses have implemented mobile device management (MDM) technology to manage all mobile devices, while a further 12 percent are testing this out.

Figure 9: Do you have any tools or processes in place for mobile use at your organisation?

No, we don't allow mobile device use at our organisation (5%)

Yes, we have mobile device management technology set up to manage all corporate mobile devices (24%)

No, we don't use MDM or EMM and have no plans to do so (29%)

Yes we have a full enterprise mobility management suite in place to manage devices and apps (13%)

We do not currently use MDM or EMM tools but have plans to do so (13%)

We are currently testing out mobile device management technology (12%)

We are currently testing out a full enterprise mobility management suite (4%)

A smaller group has taken this one step further, with 13 percent of firms currently running a full enterprise mobility management (EMM) suite, which manages everything from the devices to installed apps to networks. An additional four percent of respondents said that their firm is currently trying out EMM tools, while 13 percent said that, while they do not use MDM or EMM tools at present, they are on the radar for deployment.

However, this still leaves over a third of organisations which do not plan to implement any mobile management tools or do not enable mobile use in the workplace.

MaaS360®
by Fiberlink, an IBM company

Conclusion

Mobile has embedded itself into the workplace for organisations of all sizes and across all sectors, as devices like laptops, smartphones and tablets become the preference for staff. Even those firms that believe they do not allow mobile devices to be used for work, will no doubt find pockets of employees finding their own ways to access corporate data and applications on their own devices.

As newer categories emerge such as wearables and hybrid models, this will create further challenges and potential advantages around enterprise mobility. Firms that get their management processes in place now, ready for the next shift in mobility, will ensure that they are able to reap the most benefits from mobile in the workplace.

About the sponsor, MaaS360 by IBM

MaaS360 is the most robust cloud-based mobility management platform that spans across devices, users, applications, documents and expenses. With over one million mobile employees already being enabled using MaaS360, you can trust that our secure cloud infrastructure is ready to help you quickly and safely support your mobile operations.

- Trusted by over 6,000 customers, from small business to educational institutions, public agencies, and large global enterprises
- Supporting millions of personally owned and corporate issued smartphones, tablets and laptops
- Positioned as a Gartner Magic Quadrant leader in Mobile Device Management for past 2 years
- Named a "Champion" by InfoTech in the MDM vendor landscape report
- Backed by over 20 years of experience in enterprise mobility management

Contact

To learn more, visit **www.maas360.com**