WHITE PAPER

Global BYOD Attitudes and Best Practice for Multinational Organisations

Sponsored by: Vodafone Global Enterprise

Nicholas McQuire
August 2012

IDC OPINION

Hype surrounding "bring your own device" (BYOD) has grown considerably over the past 12 months, but global organisations in particular struggle with BYOD's business and technology complexity. Many multinational corporations (MNCs) tolerate personal devices on their networks to an extent today, but concerns over the inexorable pace of unmanaged consumer technology accessing internal systems and data are mounting.

With the globalisation of industry and an increasingly global mobile workforce that needs access to company information anytime/anywhere, a strategic view of mobility is unfolding within MNCs, fuelled by smartphone and tablet growth that exceeded 40% worldwide in 2011, according to IDC forecasts. Managed BYOD therefore — a mobile IT service backed by organisational policy and governance and part of a modern, managed workspace strategy — is emerging as a fit-for-purpose tactic to address consumerisation of IT and drive mobility benefits on a wider scale within global firms.

We estimate just 20% of MNCs have a managed BYOD programme deployed, however, as many CIOs currently lack clarity on best practice for global BYOD implementation and need help formulating practical mobility strategies and policy frameworks to manage it effectively. There is no "one size fits all" deployment model to follow either and with most MNCs not yet having an organisational mobility strategy in place, there is a real risk many could implement BYOD incorrectly, compounding risk and limiting its impact as a result.

IN THIS IDC WHITE PAPER

This IDC and Vodafone Global Enterprise White Paper explores BYOD best practice from the perspective of large multinational companies and attempts to highlight important regional and country distinctions to the topic. On behalf of Vodafone Global Enterprise, in June and July 2012, IDC talked to senior executives on BYOD strategy from over 50 MNCs across several locations around the world, including New York, London, Dusseldorf, Johannesburg, Mumbai, Singapore and Sydney. This document aims to provide critical insight gathered from these sessions including:

☑ An understanding of critical regional and country attitudes towards BYOD within an MNC context, including the perceived opportunities and challenges it poses

☑ How firms are approaching a global strategy for BYOD, particularly on issues of business case, technology, IT support and reimbursement
What are BYOD implementation best practices in terms of global and local policy, governance, data management and measurement

According to IDC’s Biannual Enterprise Mobility Survey 2012, fielded in May of this year, close to 35% of MNCs are currently evaluating a BYOD strategy. Above all therefore, this paper attempts to provide global firms with some “real world” practical direction on key tactical aspects of BYOD based on recent insight from their peers across the globe, including technology, policy and business-related considerations for effective enterprise mobility strategy, governance and risk management.

I. Prevailing MNC Attitudes to BYOD: The Opportunities and Challenges

There are many well-known and often regional and company-specific reasons for BYOD’s growing priority in MNCs. We have listed its key drivers and specific country attitudes raised in the IDC discussions below.

- **It’s happening already.** Many MNCs now recognise that personal devices connecting to their corporate networks, often in violation of company policy, is already happening. One firm in the IDC discussions noted that a recent audit revealed 10 times the number of personal devices on its network than it thought. As employee requests to connect personal iPads and other smart devices roll in to IT departments, there is also a growing perception that it cannot be stopped.

- **History in personal-liable.** US and Indian firms have a larger installed base of personal-liable devices than most countries worldwide and this is influencing MNC attitudes to the topic, especially those with headquarters and decision making in these countries. In the US, for example, over 50% of US respondents to IDC’s Mobile Enterprise Device Survey 2011 reported having over 60% of mobile users on personal-liable schemes. With a smaller percentage of international roamers and a history of offering family mobile plans as a corporate perk, US-based MNCs are the most positive on BYOD globally, especially for their domestic employees. Many US MNCs are now looking to replicate these local BYOD initiatives across their other geographies but lack an understanding of key international considerations for global deployments.

- **Executive jewellery.** Another reason for BYOD’s popularity is that it is often a “top-down” phenomenon, either formally pushed through by IT on executive order by members of the leadership team, or more commonly, informally tolerated through ad hoc support of a few key execs’ personal devices. The latter scenario, raised by Asia/Pacific firms in particular, while impossible to avoid, created “envy” in the wider organisation, giving rise to the perception that BYOD users, with better technology than the corporate standard, were “elite and favoured”.

- **Productivity.** Bullish organisations, including many US MNCs, feel that if deployed to the correct work style, BYOD can expand mobility access to a wider number of workers, enabling the organisation to capture productivity and agility benefits on a greater scale. A hotly debated topic in the IDC discussions was an untested view that BYOD users could generate one additional hour of output per day.

- **Diversity.** BYOD is also being embraced by IT departments as a tactical solution by those that have been slow to deploy a more diverse, multiple mobile operating
system (multi-OS) environment within their organisations. This was especially the case among many UK firms in the discussions, which are still highly dependent on BlackBerry devices for instance.

Employer of choice. Finally, many MNCs are prioritising a corporate objective to win “the war on talent” within their industries. BYOD is seen by some as a necessary competitive step to address employee recruitment, retention and satisfaction within their organisations.

At the same time, however, BYOD also presents significant challenges for global firms taking an international approach. The most pressing that emerged from our discussions include the following:

The business case. Contrary to a perception that BYOD is a cost saver, many MNCs, including South African and Indian organisations in particular, don’t believe BYOD saves the organisation money at all, although few track its costs directly and many don’t clearly understand overall ICT costs as an important baseline. There is a general “gut feel” among advanced MNCs that BYOD can increase mobility costs by as much as 10% with many hidden issues affecting its “true” expense, such as:

- The loss of mobile operator buying power and tax credits accrued from moving corporate plans over to employee-paid schemes
- BYOD roaming on expensive consumer tariffs and line-of-business expense-backs
- Additional software licensing fees, including enterprise mobility management software and mobile applications as devices and app usage per employee increase
- Increased administration overhead and IT support costs
- Cost of productivity loss through employees being on consumer support contracts where replacement devices are slower to source and downtime is likely to be higher than corporate support models
- Corporate WLAN investment to ensure network can handle additional devices; the network impact particularly concerned those with remote sites
- Lack of split billing services from mobile operators, roaming controls and the deployment of expense management tools to control costs

One Australian organisation noted it had embarked on a BYOD programme three years ago and had it reversed due to cost complexity. Another US MNC, which, thanks to telecom expense management (TEM) software it deployed recently, discovered that its BYOD users, representing just 10% of mobile workers, cost the firm approximately 5% more than its entire base due to a lenient expense-back policy HR had in place for employee travel. An Indian organisation said it was happy with BYOD for local use but would not consider it outside of India because its employees were not prepared to fund the roaming costs.

Information security, privacy and compliance. Managing data leakage risk from an increasing blurring of business and private data on personal devices is also a well-known concern. According to IDC’s EMEA Enterprise Mobility Survey
2012, fielded in May of this year to approximately 1,400 businesses across 18 countries, close to 50% of respondents said the potential for data leakage was the biggest concern in implementing a BYOD programme. Additionally, the “right to wipe” data on personal devices and the potential impact on user privacy it represents is far more complicated for MNCs having to consider a multitude of compliance environments, labour unions, privacy laws and in some cases cultural attitudes to personal information. Variable data privacy regulation, for instance, makes BYOD difficult to implement as a standard programme within MNCs because it requires contractual user consent to IT having a degree of access to the personal device.

Additionally, regulated industries in particular, such as finance, insurance, banking, retail, healthcare, legal and public sector, cannot afford any compromise to customer data records or compliance requirements. When putting corporate information on an employee-owned device, the corporate may be liable for loss of data, intellectual property or even earnings, if that results in loss to the employee.

There are also important regional variations when it comes to data privacy and protection regulation. In Germany, federal law concerning data protection stipulates that German company data must reside in Europe. Furthermore, German data privacy rules and work councils make the implementation of consumer technology in the workplace tricky compared with the US, for instance. These challenges are further compounded by the fact that many MNCs have not yet deployed enterprise mobility management software tools necessary to navigate these issues as well (see section III).

- **Policy and governance.** Policy is the cornerstone of any managed BYOD programme. However, MNCs struggle to centralise BYOD policy at a global level, creating in effect a central "rules of the game" that can be implemented and if required amended and localised at country level as well. How to centrally govern a myriad of local considerations across the globe, including countries with specific government regulations such as China, Russia and Germany, as well as determine which employees can access what data on personal devices from a policy point of view, are not straightforward tasks for MNCs.

- **Cultural change.** Several MNCs in Asia/Pacific noted that trust levels between senior management and employees would have to increase if their organisation was to successfully deploy BYOD. Indian firms observed that BYOD should be deployed to encourage employees to leave the office on time rather than stay late "working" while hoping to be observed by their managers. As stated earlier, Singapore, Sydney and Mumbai audiences all observed that "device envy" (whereby senior management purchase more expensive/desirable devices relative to mid/junior level employees) is an effect of BYOD that needs to be carefully monitored.

- **Global versus local decision-making challenges.** Firms in Singapore and South Africa noted that global corporate policy was not keeping pace with local market developments and felt stifled as their global HQ was not progressive in thinking around the potential of BYOD. They noted that local competitors were moving quickly and gaining early competitive advantage, so while willing to embrace BYOD, several MNCs’ global policies and strategies meant local units had little flexibility to embark on even small-scale trials or proof of concepts.
II. BYOD Approaches

There is no “one size fits all” approach to BYOD, especially for multinationals. MNCs will have their own company objectives, competitive environment, compliance regimes, risk profile, internal culture and IT strategy that determine the direction their firm will take. That said, there are some consistent attitudes emerging around approaches to key aspects of BYOD which came out of our discussions. These are summarised below.

Managed BYOD is really “CYOD”. Most current and evaluated MNC BYOD implementations concentrate on a limited set of devices and applications in a more controlled “choose your own device” (CYOD) model, with the view that more mobile devices, operating systems and company applications will be phased in over time. Few, if any, MNC BYOD deployments open the door to all devices and applications, for obvious reasons. iPhones and iPads running mainly the iOS4 and above operating systems from Apple and mobile email/calendar access are the most popular BYOD deployment scenarios today, but Android is beginning to gain ground with MNCs operating in US, China and India in particular. Most MNCs do not yet extend their programs to laptops, although many will in future as technologies such as virtual desktops (VDI) are deployed globally.

BYOD apps beyond email. While risk assessments, user profiling and data classification are critical to the process of determining which applications are relevant for managed BYOD deployments, as stated above, the vast majority of MNC implementations today concentrate on email, calendar access and browsing only as a first step. Advanced firms are now focusing on extending secure content and file management applications in evolution of this strategy. Specific business process applications, including those carrying customer data on personal devices, is a hotly debated area, with most today preferring to concentrate company mobile app strategies on corporate liable devices at least initially.

BYOD coexists with more flexible corporate liable programmes. In parallel to BYOD, MNCs are also making their corporate liable programmes more flexible as well such as offering greater device choice, mobile application support and permitting more personal application activity on corporate devices. The importance of corporate liable diversity was raised by Asia/Pacific and UK firms in particular. One firm said its BYOD programme, in operation for over a year, is small compared with its corporate liable base because its BYOD policy focuses on a limited number of devices and company applications (email/calendar only) and heavily restricts third-party apps such as Dropbox. The corporate liable programme, by contrast, offers greater device choice and support for a larger number of company and third-party mobile apps that have been more popular with employees.

IT support and self-service. IT support models for BYOD are immature and varied with no consensus emerging as to what works best. Models range from full SLA helpdesk support with break-fix, to no support at all, to tiered support based on employee grade, to even limiting BYOD support to a time-based structure per employee (i.e., 1 hour per employee per month). Despite this, most emphasised the importance of self-service tools for BYOD employees as an important requirement. These can include YouTube videos, social media pages,
Wikis, intranet FAQs, and links to forums and manufacturer Web sites, for example.

- **Reimbursement.** There is also little consistency on reimbursement procedures as well, but most have avoided providing stipends due to tax implications. Uncertain tax regulation on BYOD across countries makes stipend provisioning administratively burdensome, tricky and sometimes more expensive for MNCs. In the UK, for example, taxation is far from clear regarding BYOD smartphones, laptops and usage as some aspects of BYOD are treated by the UK government as a "benefit in kind" and subject to full VAT versus a corporate-owned device and usage of the same nature, which are exempt. What are the tax implications of BYOD and who pays it, the company or employee, has to be worked out by the BYOD programme.

Several organizations, however, observed that they did provide a deduction from an employee's salary versus cash and also have different reimbursement policies for hardware and connectivity. One organisation with a "no reimbursement" policy stressed that it had to invest in a better corporate WiFi network to cover employees on premises working out of their own pocket. Additionally, there was also concern with non-reimbursement policies that if employee BYOD costs mount, users may push back, reduce their productivity and/or shift back to corporate liable as a result.

- **Technology.** There is still a lack of maturity regarding the relevant enterprise mobility management software tools to implement effective managed BYOD programmes including mobile device management, mobile security, application management and managed services. IDC estimates that over 60% of global organisations have not yet deployed dedicated mobile enterprise management software tools within their organisations to support BYOD.

While our discussions revealed good knowledge of PC-focused tools such as desktop virtualisation, debate around the mobile environment ranged widely. Discussion covered a multitude of specific vendor solutions, requirements and tradeoffs with traditional mobile device management, sandboxing, mobile containers, mobile virtualisation and dual persona technologies, as well as the pros and cons of application-level management and browser-based identity and security controls. Additionally, expense management software was also raised as a key topic. It was felt overall that the speed of change in the mobile market was increasingly difficult for firms to pick holistic solutions, and relying on existing infrastructure such as Microsoft Exchange Activesync offered limited functionality without the support of enterprise mobility management tools, especially in terms of mobile application security. Most firms were therefore evaluating several mobile enterprise management vendors, including managed services.

### III. Implementation Considerations

Implementing managed BYOD is not straightforward for many global organisations as it involves coordination at global and local levels as well as across key business units including IT, data security, finance, HR, legal and in some cases labour unions and governments as well. That said, there are important aspects to the implementation process which many MNCs must consider. We have listed them below.

- **Policy.** As mentioned earlier, BYOD policy is the cornerstone of an effective managed BYOD programme, but many firms are wary of implementing policy
today. There are many hard considerations when putting together a global BYOD policy that factors in local needs as well as key issues such as liability, compliance and privacy, including the right to wipe information on a personal device if lost, stolen or when an employee leaves the company. There are also other potentially thorny areas in extreme cases that may also need consideration, including seizing personal devices, forensics and shared device violations.

As discussed, data privacy laws in particular make BYOD mostly an opt-in programme, as few, if any, MNCs make it mandatory to all employees. Willing participants must sign a user agreement that stipulates rules of engagement at the very least on the following items:

- Device and operating system requirements of the programme
- Application support, including file management and in some instances app white/blacklisting
- The installation of company mobile enterprise management software on personal devices including related functions such as PIN enforcement, network access controls and certificates
- Remote wipe and data backup procedures including specific language on how personal information is handled if device is lost/stolen or when employees leave the company
- IT support and break/fix procedures
- Reimbursement (including payment for insurance, hardware and connectivity)

While BYOD policy will often cover more areas than the above, much will vary from company to company. It was agreed therefore that clarity of policy, communication and education of users was absolutely critical in ensuring participants are aware of their responsibilities.

BYOD work styles. BYOD is rarely company standard across the entire organisation. Instead, it is usually a fit-for-purpose programme, coexisting with corporate liable, relevant to a willing subset of workers that have the appropriate work style requirements and risk profiles. Often, the drive for BYOD is coming from executives, customer-facing teams (such as sales and marketing), third-party contractors and younger employees. But demand is by no means universal. The discussions revealed that some workers may not want BYOD, some roles may be too high-risk or have too specific needs for it. User profiling and data classification are therefore necessary to best determine what should be a BYOD scenario and what corporate information should be accessed.

Measurement. An important aspect of BYOD implementation is how success is measured. As discussed, it is unlikely that BYOD will directly save MNCs money, though few measure it directly. The most advanced BYOD implementations therefore examine BYOD success/failure against how well it enables the business overall. These can be measured against gains around IT service levels, employee satisfaction, recruitment and retention, productivity or indeed revenue growth and customer engagement, to name a few. The IDC discussions covered heavily the importance of having in place an organisational mobility strategy
overall, enabled by BYOD, whose sole purpose is to drive the strategic business priorities of the firm forward.

- **Change management.** Cultural change management is a critical aspect of implementation raised by Indian, Australian and UK firms in particular. Several organisations said trust levels between management and employees needed to increase significantly if their organisation was to move into BYOD and an “anywhere, any device, anytime” work policy.

### IV. MNC Recommendations for BYOD Best Practice

We have highlighted a few recommendations for BYOD best practice based on the IDC and Vodafone Global Enterprise MNC discussions below. Please note that IDC intends for these recommendations to be directional rather than prescriptive and should serve as guidelines for CIOs when crafting strategies.

- **Measure BYOD against business goals with a mobility strategy.** BYOD is not an endgame itself, but rather a fit-for-purpose tactic IT can deploy to better enable a mobility and business strategy. It is unlikely firms will save money directly from BYOD, so measurement must examine how successfully BYOD and mobility overall, including coexisting corporate-liable programmes, help the business achieve its objectives. It will be required, however, to proactively monitor BYOD voice/data usage and expense via regular auditing programmes to ensure costs don’t spiral out of control. Telecom expense management software may help here.

- **Risk assess, profile users and classify data.** Not all employees and company data are relevant for BYOD, so assess with the business, the appropriate risk profiles for BYOD work styles and company data access.

- **Make corporate-liable flexible.** For companies with users that have strong compliance/regulation and security needs, task workers (i.e., field force), international travellers or employees needing mobile access to sensitive data (such as CRM applications) corporate-liable devices and/or SIMs may be preferred for these worker groups. Ensure there is relevant device and application choice for corporate-liable users as well.

- **Invest in enterprise mobility management software and have a “trusted advisor”.** Enterprise mobility management technology tools are essential to support a mobility strategy and managed BYOD implementation. Make the right investment for your needs with a trusted advisor that can help assess and implement a solution.

- **Have clear BYOD policies and set user expectations.** Managed BYOD policy will be dynamic and iterative but it is the most critical aspect to mitigate risk. Ensure BYOD users opt-in to a clear set of guidelines and are aware of their responsibilities. Key foundational policy areas include IT support procedures, remote wipe and data backup, including personal data, the installation of company management software, reimbursement, break/fix and third-party applications. Firms may also want to begin with a more controlled "CYOD" approach limited to specific devices, operating systems and applications such as email/calendar and secure file/content management as first steps. Consider
phasing in policy around additional devices, platforms and apps in time and ensure flexibility to support local country requirements as well.

 Self-service. Build a dedicated set of self-service tools beyond the standard retail channel support for BYOD users. These can include YouTube videos, social media pages, Wikis, intranet FAQs, and links to forums and manufacturer Web sites.

 Ensure cross-functional governance, possibly through a mobility CoE. A centre of excellence (CoE) for mobility, potentially led by a director of mobile strategy, could be a good way to ensure the necessary representation across countries and functional teams that managed BYOD requires. This will ensure all considerations around the business are met and potentially avoid duplication of mobile projects flying under the radar as well. It will also ensure governance in terms of strategy, standards and local needs. The CoE should assess the business risk/rewards for BYOD.

 Consider managed services. Keeping up with mobile may not be the core business of MNCs, so organisations may also want to consider a managed service. Managed services can lower costs, increase speed of deployment, and reduce capex and overall risk by providing support across the entire life cycle. Given the pace of change in mobility, companies will need a strategic partner that understands the market, can architect a solution that aligns to the business plan and mobile strategy, has specialist implementation capabilities across the diverse vendor ecosystem and can provide the appropriate support guarantees required.

 Regional recommendations. Although our conversations revealed a fair bit of consistency among MNCs across countries in terms of attitudes and approaches to BYOD, there are some important regional and country distinctions that require consideration. While US organisations are the most bullish on the topic, outside of the US, European and Asia/Pacific firms are more measured, taking into account often unique and variable cultural attitudes, data protection and privacy laws and labour unions, for instance. In Germany, local regulation and works councils can create unique implementation conditions and cultural attitudes especially in terms of data residence and managing personal and company information. In Africa, where network bandwidth is often scarce, South African firms pay attention to the network impact of BYOD especially in remote sites. Indian firms stress the importance of business case especially for international BYOD outside of India and in particular how to support a greater number of feature phones and low-end Android devices popular in the Indian market. Many Asia/Pacific organisations, especially Singaporean and Indian firms, stress the cultural change impact BYOD will have, both positive and negative, within their firms. Finally, Australian firms noted the importance of a "work anywhere" strategy that includes a more open and flexible corporate-labile programme in addition to BYOD.

Ultimately, global corporate policy may not keep pace with local needs and conditions, so be prepared to trial at local or regional level to ensure competitive advantage against local players.

 Trust and educate on security and policy. Perhaps most importantly, realise that while BYOD does raise the importance of security, security is no longer just about prevention. Modern mobile working strategies are also about a culture of providing employees with a secure working environment that enables them to do
their job more effectively with responsibility and the freedom to explore what’s possible with mobility. New trust and education levels between management and employees are therefore required to ensure employees work responsibly in accordance to policy and procedure.

V. Conclusion: A Tactical Aspect of a Business and Mobility Strategy

Employees today require greater say over technology choice within their organisations than ever before and BYOD, fuelled by the inexorable march of consumer technology in MNCs, is forcing many IT departments to reevaluate their future desktop and mobile workspace strategies. There is much hype around BYOD, however, not least because it changes the relationship between MNCs and their employees and the technology they use. Implementation is not straightforward either — there is no “one size fits all” approach to follow and its process involves mobile IT expertise, coordination across the business and a risk appetite perhaps unseen before in IT. While BYOD’s security, business case, policy and governance challenges are not underestimated, there is a growing willingness to embrace technologies such as desktop virtualisation and mobile enterprise management software and examine industry best practices to overcome them.

Ultimately, the discussions from the IDC and Vodafone Global Enterprise sessions covered in this white paper reveal that despite varying maturity levels, MNCs are not fearing BYOD but rather embracing it as a key tactical aspect of their overall mobility and business strategies. A strategic view of mobility — enabled by managed BYOD — is therefore unfolding and necessary to achieve organisational goals and compete in today's global marketplace.