

How Mobile and BYOD Are Transforming Business

Mobile technology is revolutionizing how enterprises do business. Companies implementing effective mobile strategies are increasing productivity, boosting revenue, lowering costs, streamlining business processes and improving employee morale.

Organizations with established mobile management policies see benefits in every corner of the business, including marketing and sales, services, operations, IT and even human resources. Eliminating carrier costs by establishing a bring-your-own-device (BYOD) program can save a large enterprise hundreds of thousands of dollars a year. Giving tablets to salespeople in the field can boost lead generation and revenue. Creating a mobilized workplace can attract and retain young, mobile-savvy talent.

"Companies that make strategic investments in mobility are realizing significantly higher levels of meaningful business benefits than those that do not," writes Stacy Crook, IDC's mobile enterprise research director, in a July 2014 white paper.

It's no surprise, then, that budgets for enterprise mobility solutions are expected to increase by an average of nearly 7 percent over the next year, based on a new IDG Research Services survey of more than 100 mobile purchasing decision makers. Larger enterprises (10,000 or more employees), in particular, are investing in mobile, with 64 percent of those respondents expecting an average increase of 17 percent in their mobility budgets.

Enterprises that lack a BYOD strategy are not only missing out on the many advantages provided by managed mobility, but they're also ignoring the reality of consumerization of IT in the modern workplace. "Employees are going to have mobile no matter what you do," says Jason Moody, a mobility technology specialist at Dell.

Indeed, mobile device use for work has blazed past a few early adopters to become ubiquitous. That means employees are going to use their own smartphones and tablets to do their

jobs with or without BYOD. Such user self-determination was unthinkable to IT professionals just a decade ago, but now it is a permanent challenge and opportunity for enterprises.

A boon to business

Fortunately, enterprises that have embraced the mobile opportunity by establishing formal BYOD strategies and budgets are experiencing substantial returns on their investments in a number of ways, the IDG Research Services survey shows. By far, the top two benefits of a BYOD policy, survey respondents say, are increased employee satisfaction (57 percent) and increased employee productivity (41 percent).

Both of these make sense and are interrelated. As millennials increasingly enter the workforce, they expect to use the devices,

Enterprises that lack a BYOD strategy are not only missing out on the many advantages provided by managed mobility but also ignoring the reality of consumerization of IT in the modern workplace. "Employees are going to have mobile no matter what you do," says Jason Moody, a mobility technology specialist at Dell.

apps and services with which they are familiar. "Employees' satisfaction improves when they get to use the device they're most comfortable with, one that has the features they like and know how to use," says Marcus Lane, global marketing lead for



Dell's Mobile Solutions. "There's no learning curve. Plus, if they use their personal mobiles for business use, they don't have to carry around two of the same devices."

Employees who use mobile devices get more work done because they are able to access files, contacts, data and apps from outside the office. Survey respondents report spending an average of 86 minutes each day working on a mobile device outside the office, with 28 percent using their mobile device outside the office for two or more hours daily.

This means mobile workers are getting approximately an extra 351 hours annually.* A report in The Telegraph shows that number to be as high as 460 hours a year.** "People who have a mobile device always have it with them," says Moody.

Constant access to a mobile device enables employees to check email, access files and apps, collaborate with co-workers and communicate with customers anytime, anywhere. No wonder 30 percent of the survey respondents say improved customer service has been one of the benefits of their formal BYOD policies. "Because you have a mobile device, you're able to respond more quickly to customers and give them better attention, so they're more likely to remain your customers," says Lane.

Empowering employees with mobile devices also can result in direct cost savings. An enterprise with a large staff of field workers, for example, can reduce travel expenses and even office space by enabling these employees to do their jobs without having to drive to and occupy an office to close the paperwork loop on a deal or find information for a customer.

Of course, if most of your employees have mobile devices, it's also likely that customers do as well – and this presents another way to service customers, learn more about them and retain them. "You have greater ability to know what's going on with your customers when you have mobile apps because people spend three or four times longer on a mobile app than they do on a website. So they're more immersed in the experience, and through this interaction they'll steadily provide information about their interests, preferences, online habits and even location. Mobile apps are a really good way of learning about your customer," Moody says.

Nearly all of the benefits that can be derived from and leveraged by mobile technology – higher employee satisfaction, more productivity, improved customer service and more – can spell the difference between success and failure in competitive markets. Enterprises that cede these advantages to competitors by failing to develop and implement a mobile strategy run the risk of falling behind.

Understanding the barriers to mobile

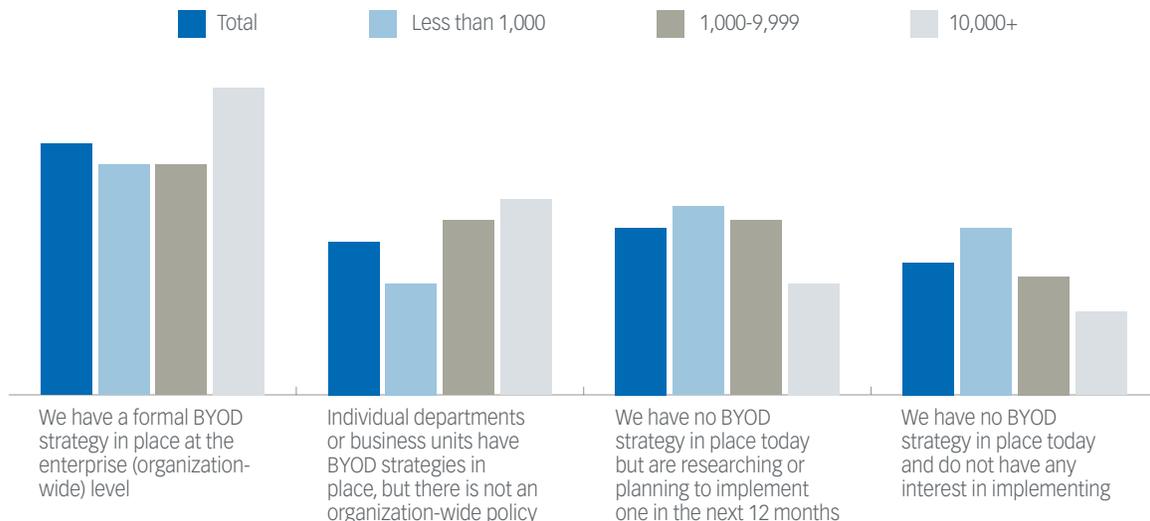
As is often the case with emerging technologies, large enterprises are far more likely to embrace mobile/BYOD than smaller organizations. Nearly three-quarters (72 percent) of large enterprises surveyed say they have a formal BYOD strategy either across the organization or within individual business units. By contrast, fewer than half (49 percent) of small and midsize enterprises report having any kind of BYOD strategy.

According to the IDG survey, mobile decision makers have nearly equal concerns about security and how to determine the return



BYOD Strategy

Large enterprises are more likely to have a formal BYOD strategy in place organization-wide than are smaller enterprises, midmarket, and SMB organizations; over half of SMB and midmarket organizations have no BYOD strategy in place, and 24% have no interest in implementing one



TOTAL BASE: 106 QUALIFIED RESPONDENTS; LESS THAN 1,000 BASE: 45; 1,000-9,999 BASE: 36; 10,000+ BASE: 25

on their investment. Respondents say the top challenges making them cautious about a mobile strategy are difficulty in measuring ROI (44 percent) and security concerns about both network and device vulnerability (43 percent each). “A lot of our customers say, ‘I just don’t know where to start, and I don’t want to invest in something that won’t do the job or is going to be out of date in six months,’” says Lane.

Some enterprise decision makers are also unsure about how to measure mobile ROI, and that’s understandable, says Moody. “It’s a very hard question to answer due to the fact that mobile implementations are different across all enterprises,” he says.

Survey respondents reported spending an average of 86 minutes each day themselves working on a mobile device outside the office, with 28 percent using their mobile device outside of the office for two or more hours daily.

“Many organizations will measure mobile ROI by how many IT resources it takes to implement and manage a new strategy or solution – they want something that takes fewer resources. Others will measure it in energy costs, how much faster they’re getting data or how they can capture all the big data generated by mobile and do data analytics.”

Carrier costs can be yet another way to measure mobile ROI and reap savings. Organizations used to rely on IT for Internet access, but with BYOD and mobile, that has been handed off to individual users and their relationships with public carriers. “For a large enterprise such as Dell – we have 100,000+ employees – the savings alone in carrier costs from enabling BYOD ended up being about \$1 million,” says Moody.

Even as the competitive and cost advantages of managed enterprise mobile become increasingly clear, security concerns make many IT decision makers hesitant to commit to a mobile strategy. The need to improve endpoint security is the top driver of a formal BYOD policy for respondents (48 percent) whose organizations have yet to implement one. They worry about mobile devices being lost or stolen. They fret about employees connecting to the network using unsecure public Wi-Fi, or failing to use passwords or encryption. They keep their eye on

servers with weak access controls and worry about mobile apps containing malware.

Mobile applications, in particular, pose a danger to enterprises, according to research firm Gartner, which forecast in September 2014 that more than 75 percent of mobile security breaches through 2017 will be due to mobile app misconfigurations, “rather than the outcome of deeply technical attacks on mobile devices.”***

The emphasis on endpoint security makes perfect sense because employees can lose mobile devices, fail to activate remote lock and wipe features, and install apps that often require intrusive permissions. These permissions can include authenticating password accounts (which could enable a rogue app to steal a password), reading log data and contacts, and altering system settings.

All of these activities are far more likely to occur in an enterprise that does not have a formal BYOD policy, which typically includes extensive employee training in mobile device security features and best practices. As Moody notes, “Users are going to have mobiles anyway, no matter what you do.”

Ironically, too much mobile security can lead to potential security breaches. This happens when enterprise efforts to secure mobile data become so onerous that users engage in workarounds.

“If IT becomes a roadblock, people create ‘shadow IT’ to go around them,” says Moody. “They say, ‘I’m going to create a cloud share and we’re going to get our work done and make our deadline.’ Then all of a sudden you have data sitting out there somewhere because users have gone around you. The best solution is to understand what applications and services they’re using to get their work done and provide those on personal devices, integrating them with users’ existing enterprise productivity and collaboration tools.”

Mobile vendor wish list

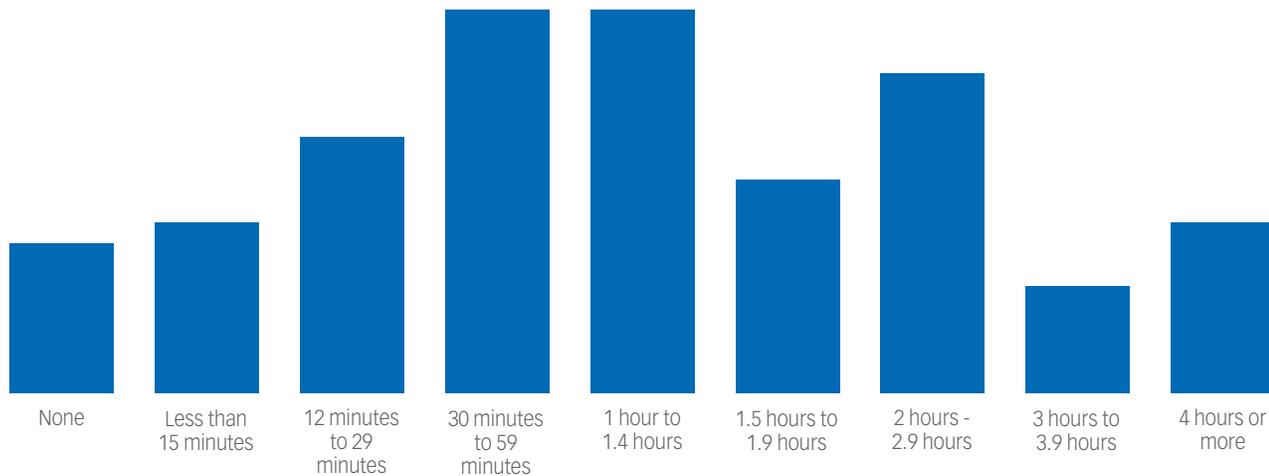
Though many organizations have concerns about mobility and BYOD, that doesn’t mean there aren’t solutions out there to address those concerns. So not surprisingly, the most important consideration by far for the survey respondents when selecting an enterprise mobility vendor is how effectively it handles security. Five of the top seven priorities in choosing among mobility vendors involve how well each vendor protects enterprise networks and data. Eighty percent of respondents say it is extremely important or very important that a mobile vendor can implement secure access/policy-based controls.

Other security features deemed extremely or very important by respondents are: endpoint/device encryption (69 percent), secure mobile browser (68 percent), secure file manager (66 percent) and isolation of enterprise apps and data on personal devices (60 percent). It also could be argued that policy management/compliance (69 percent) is related to security in that it’s meant to protect the enterprise.



Time Spent Out of Office Working on Mobile Device

On average, respondents spend an hour and 26 minutes per day working on their mobile device away from the office; organizations that list mobility as a critical or very important enabler of productivity spend nearly twice as long working on their devices away from work (1 hour 43 minutes) than do those citing not very or not at all important (59 minutes)



TOTAL BASE: 106 QUALIFIED RESPONDENTS

IT decision makers must further consider a wide range of integration issues and business functionality requirements. How well a mobile vendor enables business communications – specifically, email, calendar and contacts – is rated extremely or very important by 75 percent of survey respondents, making it the No. 2-ranked mobile vendor capability.

The emphasis by survey respondents on security, communications and collaboration clearly shows that enterprises of all sizes seek an enterprise mobility vendor that not only can effectively protect devices, data and networks, but also can enable users and the overall business to achieve greater productivity, efficiency and agility. “Customers need a lot more than to figure out how to equip some handsets,” says Lane. “It’s about finding a partner who’s going to provide them with an integrated solution – with everything from management, security and tools for productivity and collaboration – for all the segments of the enterprise that mobility affects.”

By gauging the needs of your employees through surveys about work patterns and behavior, the pieces of the puzzle will become clearer. For example, if employees use Android, iOS and Windows devices, it’s imperative that mobile device management (MDM) or the secure workspace solution selected provides support for all these platforms.

If an enterprise has ambitious expansion plans, mobile decision makers should look for a mobile solutions vendor that can scale to meet the growth of the business. To help ensure data protection, enterprises should consider whether a vendor’s

software includes built-in encryption and if it provides backup and restore functionality for device data stored in the cloud. And if IT prefers the ability to remotely configure and support mobile devices, an enterprise should look for a solution vendor offering strong remote management capabilities on personal devices.

Once the productivity needs of employees and the requirements and features for securing mobile devices and data are well understood, it becomes easier for enterprise decision makers to select the best tools for managing and taking full advantage of mobile technology.

The challenges, however, are not the point. Mobility is fundamentally changing the workplace, and anything that powerful and sweeping will invariably be disruptive. It’s not a question of if you will embrace mobile. It’s a matter of when and how. ■

*The 351 hours were calculated thusly:

Five days/week x 52 weeks = 260 days – 10 days (vacation) – five holidays (Labor, Memorial, Thanksgiving, Christmas, 4th of July) = 245 days
245 days x 86 min/day = 21,070 min = 351 hrs = 14.625 days

**The Telegraph, <http://www.telegraph.co.uk/technology/mobile-phones/9646349/Smartphones-and-tablets-add-two-hours-to-the-working-day.html>

***Gartner Sept. 14, 2014 press release, <http://www.gartner.com/newsroom/id/2846017>

