dimension data

Secure Mobility Survey Report

A critical gap exists between the enterprise mobility vision and real-world implementations

introduction

Enterprise mobility and trends like bring your own device (BYOD) aren't just hot topics of conversation.

According to the over 1,600 IT and security professionals we surveyed, mobility is a top priority for most IT departments.

Unfortunately, there's a critical gap between the vision these IT leaders have for enterprise mobility and the real-world implementations.

The insights gathered from IT professionals in the Americas, Asia Pacific, Europe, the Middle East, and Africa demonstrate that organisations from around the world share many of the same priorities, challenges and risks.

vision versus execution

A critical gap exists between the enterprise mobility vision and real-world implementations

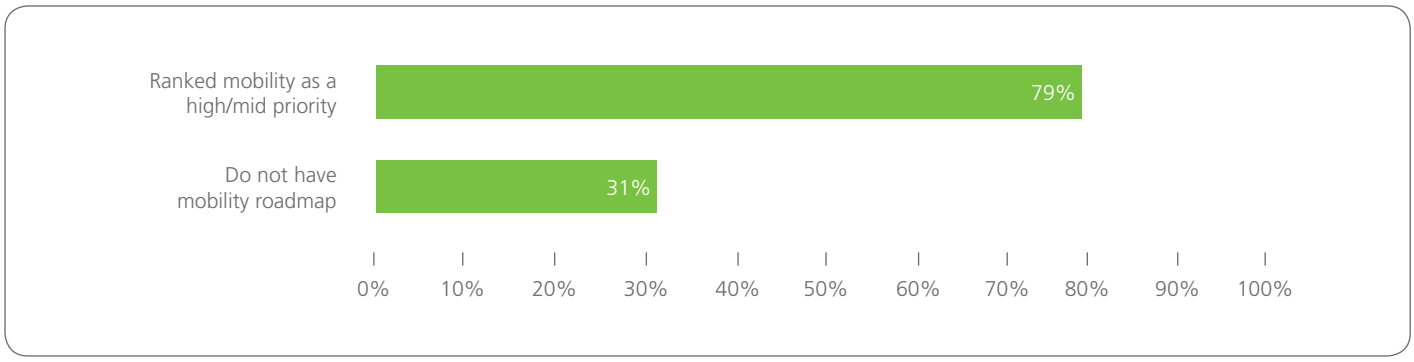
An IT roadmap that integrates with a business's operational goals and the organisation's existing IT infrastructure – one that provides for necessary resources and budget and also highlights potential challenges – makes the difference between a successful implementation and being derailed by unforeseen problems. This is especially true when it comes to mobility, which is particularly complex and touches most parts of an organisation's network infrastructure. For this reason, it isn't surprising that of the **79% of IT leaders who classify mobility as a top priority, 69% already have a roadmap in place.**

What is surprising, however, is that two critical issues are not being addressed by a vast majority of those who are implementing a strategic mobility roadmap. **Only 29% of those who are implementing their roadmap have tested how well their core applications work on mobile devices and 32% have conducted a security audit of applications touched by mobile devices** – even though **71% of them named data security as their greatest mobility-related concern.**

Testing how well core applications work on mobiles devices and conducting security audits of these applications are critical building blocks for a successful mobility roll-out.

> **'Devices must be configured and managed with information assurance controls commensurate with the sensitivity of the underlying data as part of an overall risk management framework.'**
>
> **IT Manager – Large grocery store chain, USA**

Global analysis – 1,622 respondents



Without taking these steps, IT departments will most likely deliver sub-optimal end-user experiences that will inhibit adoption – and, just as importantly, they'll miss out on the chance to proactively identify and solve security challenges before they become threats.

It's clear that mobility is a top priority for IT leaders and that most have a clear vision of the role mobility can and will play in their organisation. Overall, they see both the opportunities and the risks. That said, responses to the survey point to a gap between that overall vision and the likely real-world outcomes organisations will face – given that a number of crucial initial steps that can ultimately save time, reduce costs, and, most importantly, ensure security are typically not taking place.

concern outweighs action

The vast majority of respondents (82%) indicated that employees at their organisations are using personal mobile devices for work purposes. Analysts advocate that organisations must have a clear mobility strategy that ensures mobile technology is an investment that works hard to deliver business value and meet the demands of an increasingly mobile workforce. To some extent, organisations are starting to listen to the analyst community because today, **55% of the organisations surveyed have a mobility roadmap of some kind.**

But the findings of this survey also indicate that many of those organisations that have designed and are implementing a mobility strategy haven't followed further analyst advice: to make time to determine precise mobility requirements and identify IT policies required to control deployments, manage risks and support users before they deploy.

Given the explosion of personal mobile devices being used for work, the importance of data security and privacy concerns is not lost on IT leaders. **Over 77% of respondents stated that information security and privacy concerns are the greatest challenge they expect to face when they build and implement their mobility strategy.** The concerns of these IT leaders reflect the real-world findings of Dimension Data's most recent Network Barometer Report. The Report is based on data collected on devices throughout the infrastructures of over 300 leading enterprise-class networks. This is not an opinion-based analysis; it's data recorded directly from the devices themselves. The 2013 Report discovered that 67% of all devices, all of which are on mature networks, carry at least one known security vulnerability – which adds an increasing amount of complexity and opportunity for intrusion. It's not surprising to learn then that only **27% of respondents feel that they have well-defined network policies in place for mobility.**

27% indicated they have well-defined network policies for mobility.

Employees use their devices to access our systems on their own. It's nearly impossible to stop. We need to establish clear policies to increase control, improve visibility and decrease risk.

Over 90% of respondents agreed with this statement. **But, only 27% indicated they have well-defined network policies for mobility.**

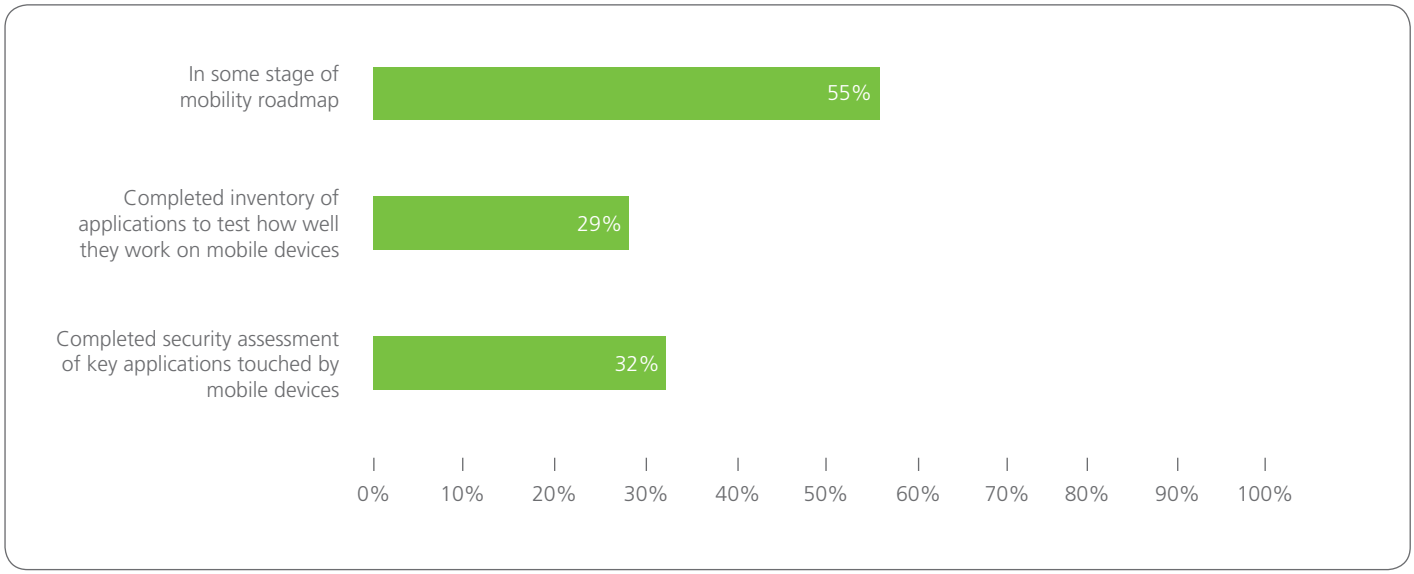
knowing where to start

Given the security issues found on the vast majority of devices within mature networks, IT leaders are correct to be concerned about data security and access control issues relating to mobility. **The importance of protecting company data is a top mobility priority for 71% of respondents, while 65% identified access control as their top priority.**

What is surprising, given the extent to which they recognise the risk, is that the area where IT leaders have the greatest amount of control – **conducting security audits of applications touched by mobile devices – has not been a priority. Only 32% of respondents have taken that step.**

According to Dimension Data's Tim Boyd, 'As organisations have seen a rise in employee-owned devices requesting access to network resources, it can be difficult to know where to start. Securing critical data and your infrastructure is not just a "I want to get my iPad on the network" problem. One must look at the greater scope of enterprise mobility and consider many facets including security policy, risk assessment, costs of operational support, and the effects on application service delivery and employee productivity. Ultimately the business case must establish a balance that maximises the utility of an organisation's resources for each of the stakeholders involved.'

Global analysis – 1,622 respondents



productivity, the user experience and security

Real-world employee productivity improvements, user experience and security are not meeting expectations.

Over 90% of respondents believe that employees will use their personal mobile devices to access enterprise systems on their own and that IT does not have the capability necessary to stop this activity. IT leaders believe clear policies are needed to increase control, improve visibility and decrease risk.

'A usage policy needs to have clear, precise statements about the rights and duties of both the employee and employer regarding ownership, access and data removal of BYOD.'

Independent security specialist, Switzerland

However, **80% of respondents also seek to create a positive mobility experience for employees, to help increase productivity.** To a large extent, employee experience is important to IT leaders because **79% of them recognise that an increase in worker productivity is the greatest benefit offered by mobility**.

Boyd adds, 'When compounded, the benefits of an efficient and open enterprise mobility strategy that has adequately addressed business policy, and limited risks, yields a much more competitive, profitable, and agile organisation.'

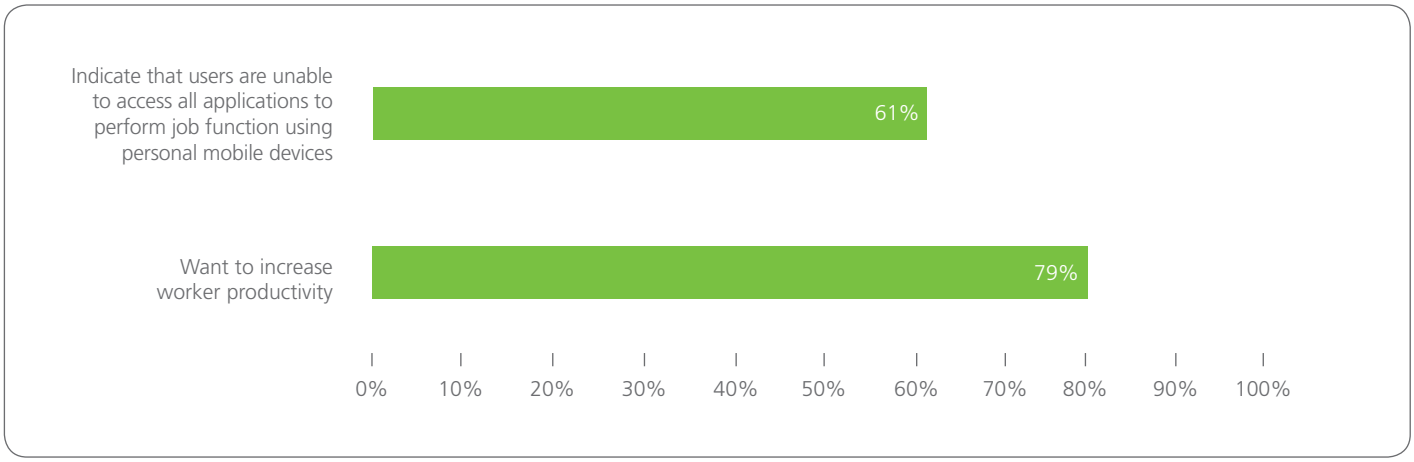
IT leaders don't only view increased productivity in terms of gaining better utilisation of existing resources. Mobility isn't just about enabling employees to do more work, faster than before. A majority of IT leaders also want to embrace mobility to enable workers to resolve client issues more quickly and increase overall client satisfaction.

Instant messaging applications and web collaboration tools have been optimised the most at 47% and 42% respectively, but 61% of respondents indicated that employees are unable to access all the core applications they need to perform their job functions from their mobile devices. Furthermore, although 53% of corporate headquarters are optimised for mobility, the intranet is optimised for only 41% of those organisations.

Much of the focus on mobility strategy and implementation seems to relate to internal communication: individuals are better able to take meetings using their mobile devices, but the ability to have access to the applications needed for decision-making and to collaborate effectively are not enough of a priority to have a substantial impact on employee productivity or business agility. It's good that people can access a corporate phone book, respond to email, and make use of WebEx using their mobile devices. However, without optimised access to their business applications, employees are still deskbound for any work that requires mission-critical data, and analytics that can transform an impromptu discussion into a hands-on workshop or a negotiation that closes a deal.

non-corporate applications and user support

Global analysis – 1,622 respondents



Perhaps because of the limited investment in enabling employees to access the business-critical applications needed to perform their job functions, **24% of respondents indicate that their organisation allows them to download non-corporate applications to increase productivity.** This is another example of where the gap between the overall vision and the way in which it's typically executed makes it difficult for organisations to achieve their goal – while at the same time creating new and often undetectable security vulnerabilities.

Overall, organisations want to increase employee productivity. Instead of focusing on enabling workers to take full advantage of corporate-approved applications with their mobile devices, a large number of organisations are allowing workers to select applications on which they may place corporate information.

It goes without saying that an organisation should be aware of the applications that are on the network and that are accessible via mobile devices. This helps organisations monitor user adoption of mobile enterprise applications, track new applications coming into the enterprise and identify when rogue applications are introduced into the system. Although this is a vision with which most everyone would agree, analyst reports indicate that enterprises are, more often than not, aware of only 80% of the devices on their network. Worse, those unknown devices inside the perimeter of the network are unmanaged and give users access for which they may not be authorised.

Surprisingly, **29% of IT leader respondents state that non-employees and guests are able to obtain limited access to the network from their personal mobile devices.** Given the difficulty of identifying new applications placed on the network, non-employee and guest access to the network increases the importance of making sure that security experts are intimately involved in the development of an organisation's mobility strategy.

When new technology enters the corporate environment and is used by workers daily, the level of support given to employees becomes a critical issue for adoption. Also, if support is limited – particularly if the procedures and processes for providing that support are not fully defined – it can take IT longer than usual to solve end-user issues, which in turn creates a backlog of issues to solve. In the case of mobility, dedicated support resources seem to be an afterthought – which is remarkable given the level of mobile devices being used by employees today. **Only 35% of respondents have addressed troubleshooting mobility at all** – either with a help desk that's meant to support all issues or a specialised resolution team.

According to Boyd, adoption of an enterprise-wide mobility strategy often stalls as organisations consider the daunting task of providing support, and its associated cost. Often, internal support for personal mobile devices is skipped entirely, exposing the organisation to a host of risks as employees, and even business units, provision their own services to support productivity. Enlisting the powerful tools available for mobile application management, mobile expense management and mobile device management can significantly lower the burden and costs of support- and troubleshooting-related challenges. When coupled with employee education, training and awareness, based on a foundation of an effective security policy, supporting a sound enterprise mobility programme is well within reach.'

mobility and security from the top down

Understanding the opportunity and the real risk

The threat to an organisation's proprietary information is certainly foremost in the minds of IT and security leaders. Interestingly, **71% of respondents indicated that their business leaders view employee utilisation of personal mobile devices as potentially dangerous, costly and not business critical.**

'For most business, it's not case of if, but when personal mobile devices in the workplace will be business-critical,' comments Boyd. 'As an increasingly more technology-aligned workforce evolves, the effective and seamless use of personal mobile devices will help both attract and retain top talent. As a by-product of staying ahead of the enterprise mobility curve, companies are quickly coming to realise that empowering the mobile worker pays dividends in terms of worker productivity and efficiency. Efficient anywhere, always-on access between employees, partners, clients, and suppliers keeps today's high-performance organisations ahead of their competition.'

When asked about the level of agreement to the statement, **'Security risks generated by BYOD are understood by IT, but not business leaders', only 30% of respondents agreed to a great extent.** 'We see that many organisations are starting to understand the risk associated with BYOD', says Boyd. However, the extent and depth of the risk has not been measured adequately against business policy because many organisations have yet to evaluate the impact of mobility beyond the device. Having rogue, inadequately protected, and unknown devices on the network is really just a slice of the risk landscape. Organisations must also consider their sever and application infrastructures along with data protection against, left, loss, or corruption, as users, data, and devices traverse the network. Not considering the entire enterprise mobility landscape has led to an assumption of risk that is often grossly miscalculated, leaving the organisation exposed to financial and reputational threats.'

61% of respondents indicated that employees are unable to access all the applications needed to perform their job functions from their mobile devices.

In total, **42% of respondents think it's important to engage IT to deter email and network access via mobile devices,** and **67% stated that data security is the most important BYOD-related policy a company should put in place.** On the one hand, there's considerable concern regarding data security. On the other, there's an equally strong belief that mobile devices have the potential to substantially increase worker productivity. As a result of this tension, a large majority of organisations have mobility roadmaps and 79% of IT departments viewing mobility as a top priority … but at the same time, very few organisations are dedicating enough resources to fully enabling users to leverage existing business applications in ways that substantially increase productivity. Also, very few organisations are conducting appropriate application testing, or making mobile infrastructure design decisions – making them even more vulnerable than they may realise.

Once mobility is integrated into an organisation, employees' ability to access the tools they need to do their jobs anywhere and at any time will be a benefit to both the organisation and its employees.

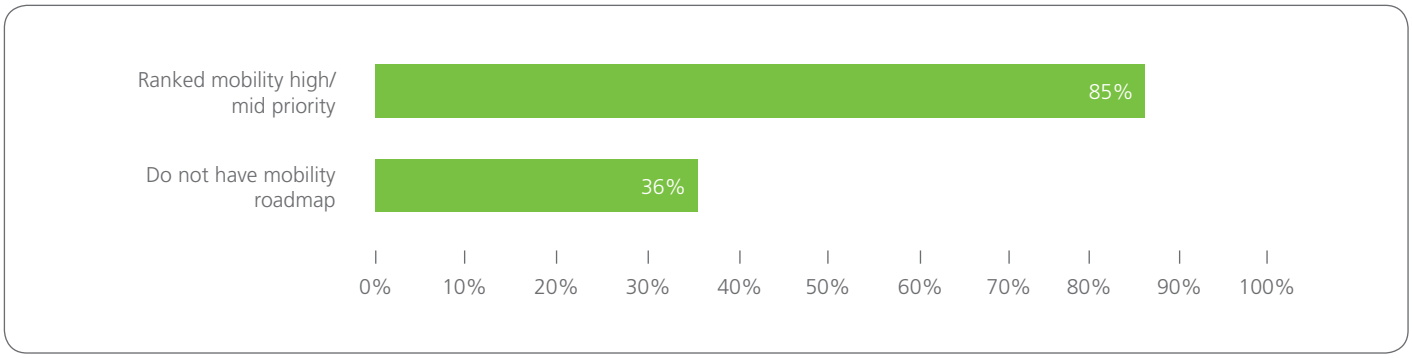
local insights

Local insights – Europe

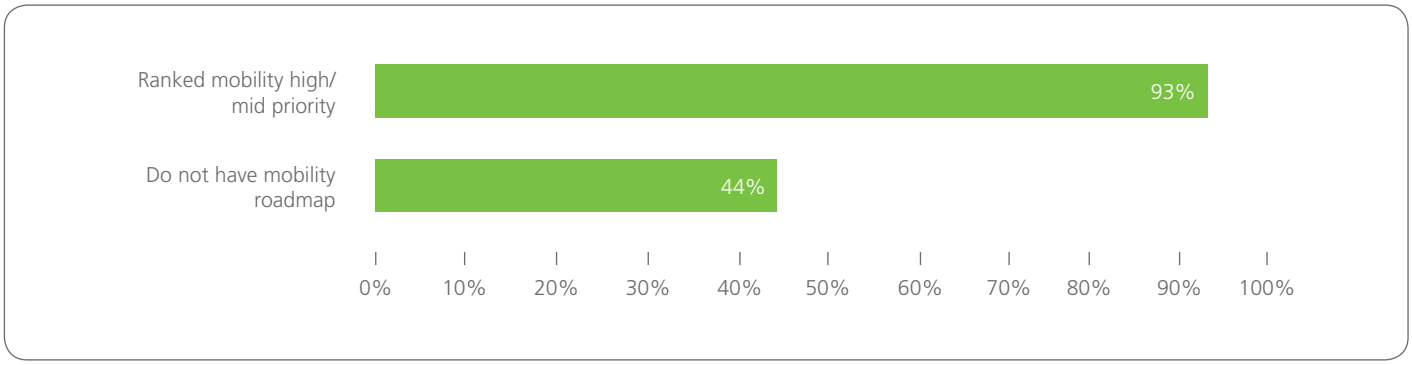
For survey respondents in Spain, mobility is a higher priority than it is for their European and global counterparts. However, organisations in Spain are less likely to have a mobility roadmap than their counterparts across Europe and around the world. Spanish IT leaders are also outranked by their global counterparts when it comes to the completion of both applications inventories and security assessments.

A mobility roadmap that governs how users access corporate data and applications is necessary to safeguard the network, protect company materials and optimise corporate applications to help employees get the best benefit of mobility. For those organisations choosing not to support or acknowledge employees using personal devices to access the network, having a well-defined network policy for mobility is imperative.

Europe



Spain

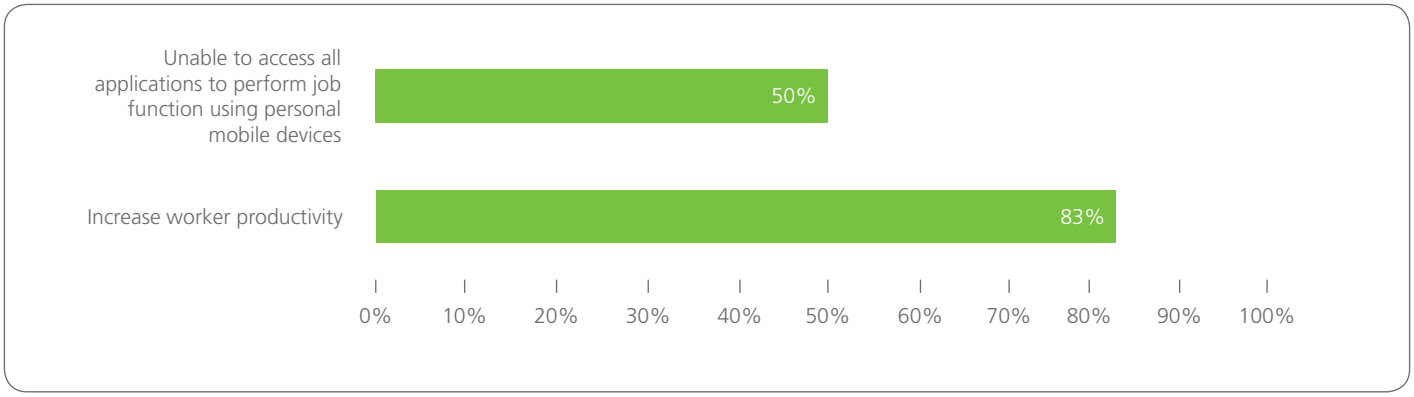


‘A mobility policy should be monitoring the use of corporate data, while maintaining a user-friendly interface.’

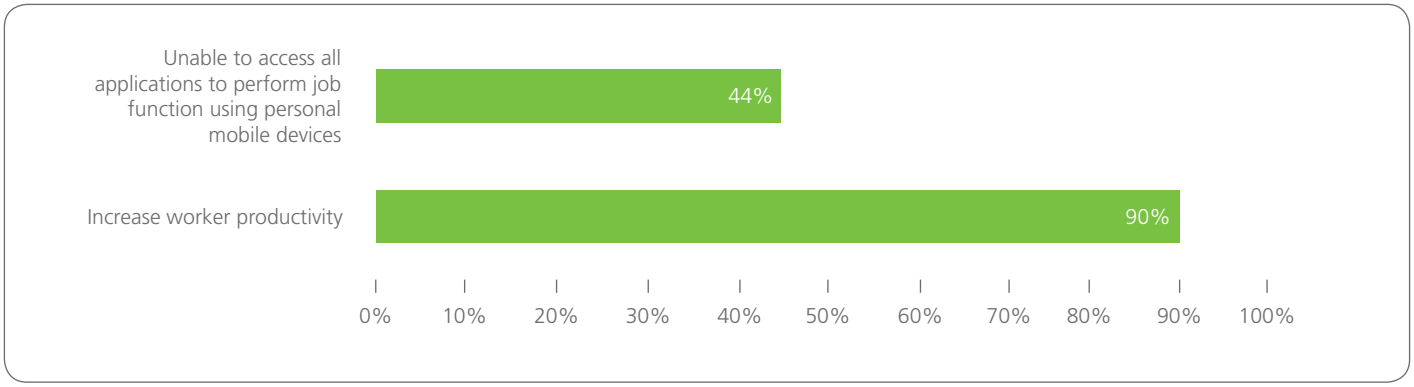
Project Manager, Spain

local insights

Local insights – Americas



US



Prior to a executing a roadmap and strategy, assessing what applications need to be optimised and secured for mobility is critical to ensuring that plans accurately capture everything from potential network enhancement to management and control requirements. Although **90% of survey respondents in the US believe that increasing worker productivity is the greatest business benefit** – more than their global or regional counterparts across the Americas – they're also less likely than other countries to provide employees with access to all the applications they need to perform their jobs, using their personal mobile devices.

Having a support team to mitigate issues and making sure that guests and non-employees have access to the network are just some of the important things organisations need to be thinking about and addressing.

Once mobility is integrated into an organisation, employees' ability to access the tools they need to do their jobs anywhere and at any time will be a benefit to both the organisation and its employees. Sales teams in the field, employees with flexible work schedules, and mobile workforces – as well as many other areas of the business – will have enhanced capabilities and improved work-life balance.

local insights

Local insights – Asia Pacific

For the 382 respondents in Taiwan, the country with the highest response rate, mobility is a lower priority than their Asia Pacific and global counterparts. This might explain why a much higher number of these organisations do not have a mobility roadmap in place and believe they do not have well-defined policies around mobility. However, a roadmap and policies are a necessity for these organisations, who are indicating a higher percentage of their employees are utilizing personal mobile devices for work in some capacity. This presents quite the problem for Taiwan organisations who see the benefits of mobility as increased worker productivity and resolution of client issues as the greatest benefits of mobility and yet have almost double the amount of respondents unable to access all the applications they need from their mobile devices to properly perform their job functions. Finally, with 67% of these organisations lacking dedicated resources to help troubleshoot BYOD-related issues, long-term security and success are at risk.

A mobility roadmap that governs how users access corporate data and applications is necessary to safeguard the network, protect company materials and optimise corporate applications to help employees get the best benefit of mobility. For those organisations choosing not to support or acknowledge employees using personal devices to access the network, having a well-defined network policy for mobility is imperative.

Having a support team to mitigate issues and making sure that guest and non-employee have access to the network are just some of the important steps organisations need to be thinking about and addressing.

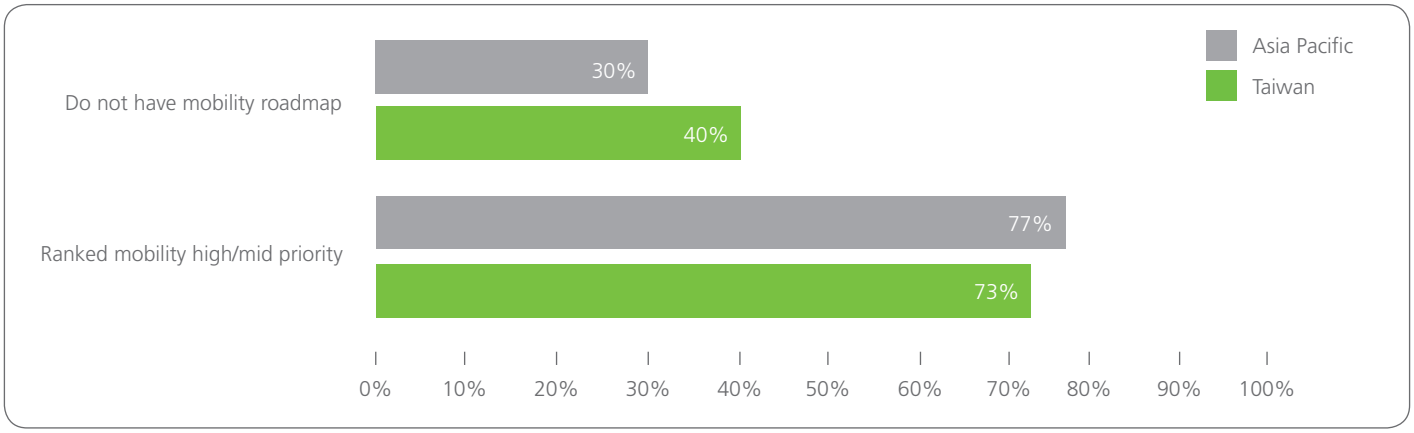
Once mobility is integrated into an organisation, employees' ability to access the tools they need to do their jobs anywhere and at any time will be a benefit to both the company and its employees. Sales teams in the field, employees with flexible work schedules, and mobile workforces – as well as many other areas of the business – will have enhanced capabilities and improved work-life balance.

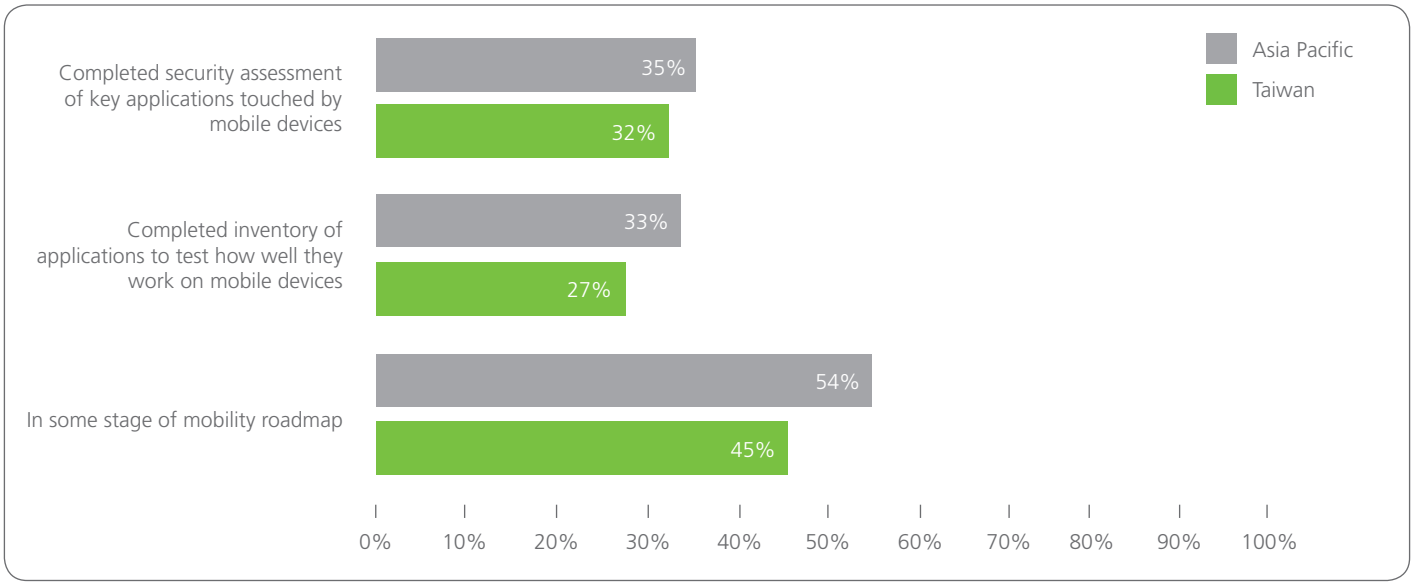
'BYOD should be based on corporate information security policy management, and provide the necessary connectivity services and security.'

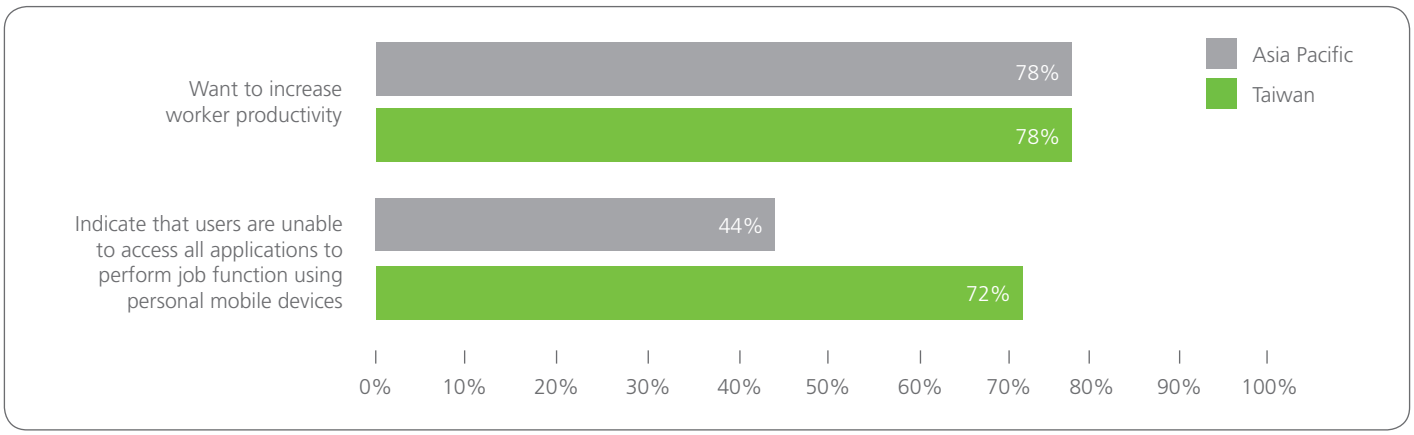
Respondent: High commissioner, Taiwan

local insights

Taiwan and APAC analysis – 382 and 1,013 respondents

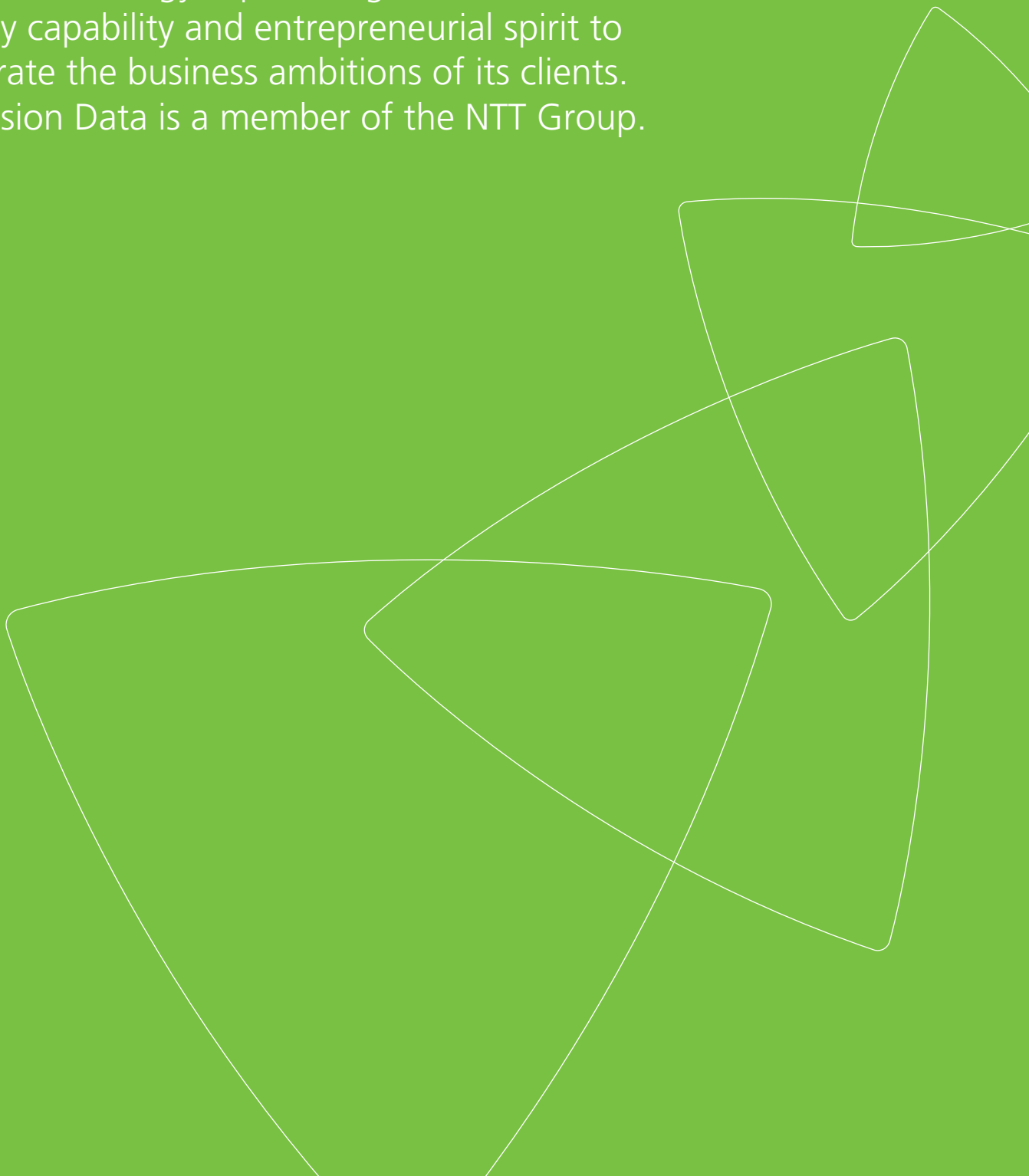






About Dimension Data

Founded in 1983, Dimension Data plc is an ICT services and solutions provider that uses its technology expertise, global service delivery capability and entrepreneurial spirit to accelerate the business ambitions of its clients. Dimension Data is a member of the NTT Group.



dimension data

Middle East & Africa

Algeria • Angola
Botswana • Congo • Burundi
Democratic Republic of the Congo
Gabon • Ghana • Kenya
Malawi • Mauritius • Morocco
Mozambique • Namibia • Nigeria
Oman • Rwanda • Saudi Arabia
South Africa
Tanzania • Uganda
United Arab Emirates • Zambia

Asia

China • Hong Kong
India • Indonesia • Japan
Korea • Malaysia
New Zealand • Philippines
Singapore • Taiwan
Thailand • Vietnam

Australia

Australian Capital Territory
New South Wales • Queensland
South Australia • Victoria
Western Australia

Europe

Belgium • Czech Republic
France • Germany
Italy • Luxembourg
Netherlands • Spain
Switzerland • United Kingdom

Americas

Brazil • Canada • Chile
Mexico • United States

For contact details in your region please visit **www.dimensiondata.com/globalpresence**

www.dimensiondata.com