Embracing Enterprise Mobility in Asia/Pacific: How Ready is Your Organization?

Sponsored by: Samsung

Ian Song  Charles Reed Anderson
August 2013

IN THIS WHITE PAPER

Most Asia/Pacific organizations’ mobility initiatives today are reactionary efforts to the emergence of the bring-your-own-device (BYOD) trend in the workplace. Although enterprises increasingly appreciate the need to move beyond just device-level security and management, the overall understanding of value delivered through mobility is still severely lacking. BYOD is one of the drivers behind most enterprise mobility investment decisions, and the journey is long and challenging. So far, most of the initial implementations tend to be in response to either employee demand or competitors’ moves, and are not undertaken with a proper mobility strategy or consideration for the security risks. The lack of understanding of enterprise mobility not only limits the addressability of mobile devices, but also produces low satisfaction levels among users. Additionally, enterprises without a strategy run the risk of investing in solutions that may not address their growing mobility needs. There are three areas that present challenges to enterprises:

- **Securing Mobility.** Mobile security is, perhaps, the most important aspect of mobile management. Yet, organizations today tend to address security from a device-centric angle. Given the rapid evolution of consumer mobility, simply managing the devices is a zero sum game. Instead, enterprises should take a more holistic approach to security with solutions that address device, location, service, network, infrastructure and user security.

- **Enterprise Mobility Ecosystem.** The enterprise mobility ecosystem is a complex environment where hundreds if not thousands of mobile products and services reside. The challenge for the enterprise is that a robust and secure solution will involve integrating multiple products from multiple vendors into a single solution. The inherent complexity may slow down overall adoption.

- **Mobility Maturity.** As mobility is becoming an integral part of the IT and business strategy, it is important to know which stage of the mobile evolution one’s organization is currently in. Trying to assess the maturity level is further complicated by the different demographics and levels of IT capabilities across the Asia/Pacific region, from the developed economies of Singapore and Australia to the developing economies of Malaysia and Thailand, as well as the industries in which these companies operate.

This IDC white paper will examine the current state of enterprise mobility in Asia/Pacific, focusing on the different stages of mobility adoption and maturity as
enterprises transition from simply managing BYOD to embracing mobility. The white paper is divided into several sections that discuss mobile security, enterprise mobility ecosystem and the IDC Mobility Maturity Model, all of which are important to understand in order for enterprises to assess the need for mobility as well as their capabilities to address it. Finally, IDC will offer a framework that enterprises can use to identify the opportunities that mobility brings as well as investments needed to realize those opportunities.

SITUATION OVERVIEW

Onramp to Enterprise Mobility

Mobility has become an integral part of consumers’ everyday lives. The proliferation of smartphones and tablets has given birth to new models of computing that were impossible just a few years ago. While smartphones and tablets are the catalyst for the BYOD movement, applications and services are the fuel feeding the BYOD fire. The mobile transformation is the evolution of consumers embracing the ecosystem of devices, applications and services. And the challenge for enterprises and their IT departments are no longer just about securing and managing mobile devices itself, but rather the entire consumer-based mobility ecosystem. Concurrently, enterprises are also beginning to realize the value they can harness from a properly secured and managed mobility ecosystem that mimics the usability and experience of the consumer counterpart. And this is how the consumerization of IT and BYOD has become the onramp for enterprise mobility.

Security is Crucial for the Mobility Journey

Organizations need to prioritize security when it comes to mobility. However, addressing mobile security does not mean only looking at the device itself. Rather, organizations need to approach mobile security holistically by evaluating multiple factors:

- **Devices.** Device security and management is one of the most important aspects of enterprise mobile security. Solutions securing the device should provide capabilities such as, but not limited to, root/jailbreak detection, control of hardware functions, location detection and remote data management.

- **Applications.** Application security and management ensure that mobile devices and sensitive information are not compromised due to security flaws of applications residing on the device. Basic application security should provide black/whitelisting of disapproved/approved applications in the corporate environment and centralized management and provisioning of applications. More advanced methods may include app-wrapping that bake security and management into the applications itself.

- **Services.** Consumer-level mobile services may provide convenience, but they are a nightmare in terms of security. Enterprises need to evaluate different mobile services and decide if they pose security risks. At the same time, implementing enterprise-level mobile services such as cloud storage and social
media, in which security and management are ensured, may be an acceptable alternative.

- **Network.** Mobile devices have multiple ways to access network resources. Enterprises must ensure that remote access, access control, network traffic management, encryption and authentication capabilities are in place and designed to handle mobile devices and ensure the security of data in transit. Additionally, investment in connectivity management can further ensure security.

- **Infrastructure.** Aside from network infrastructure, enterprises should be mindful of the security of other datacenter infrastructure components. Mobility creates additional avenues to access data at rest that reside on the datacenter infrastructure. Ensuring the security of the infrastructure in the age of mobility is paramount due to the high value of data residing in the datacenter.

- **Users.** End users will always be the weakest link in any enterprise's security solution. Mobile devices and BYOD is a deadly combination because the users now have the tools (and know how to use it) to do whatever they want in the enterprise. Securing the users through communication and corporate policies could be very effective in minimizing the security risks posed by uninformed users.

---

**Emergence of Choose Your Own Device**

Despite holistic security and management, BYOD will always pose security issues. This is the nature of personally-owned device, where a single device serves multiple purposes. A BYOD smartphone will have the employee's personal as well as corporate data and applications. Managing BYOD is a compromise between the user and IT because IT cannot deliver the devices, applications and services users want. At the same time, IT is hesitant to deliver sensitive application, data and services through BYOD platforms because of the inability to fully secure the personal side of BYOD. Additionally, there will always be a layer of confusion of device and data ownership and liability under the BYOD model.

In many companies, a new trend is emerging. Eligible users are given a choice of devices that they can use for work, also referred to as the "choose your own device" (CYOD) model. CYOD is a new spin on the traditional corporate-liable mobility model in which the enterprise takes full ownership of the device; the exception is that IT now owns and manages popular smartphones and tablets users would actually want to use. Under CYOD, there is no confusion of device/data ownership, and the IT department can fully secure the devices. Additionally, IT can deliver more services to mobile device because there are much less underlying security flaws compared to BYOD. In fact, IDC forecasts that in Asia/Pacific, BYOD rates in developed countries will eventually level off as more enterprises adopt the CYOD model.

---

**Move Beyond Security and Devices**

Enterprises in the Asia/Pacific region have been overly focused on addressing tactical challenges brought on by BYOD, resulting in a tendency to associate enterprise
mobility with securing and managing BYOD. However, BYOD management is just a part of the larger enterprise mobility ecosystem.

FIGURE 1

Enterprise Mobility Ecosystem

End Users | Applications | Devices | Connectivity | Security | Middleware | Infrastructure

- Enterprise Customers
- Suppliers
- Employees

- Games
- Social Media
- Tablets
- Handsets

- Wi-Fi
- 3G
- LTE
- NFC
- WIMAX
- WiMAX
- Other

- Secure Remote Access
- DLP
- 2 Factor Authentication
- Encryption
- Mobile Device Management
- Mobile Application Management

- Internet
- E-mail

Source: IDC, 2013

The enterprise mobility ecosystem, as shown in Figure 1, illustrates a complex environment in which hundreds if not thousands of mobile products and services reside. The challenge for the enterprise is that a robust and secure solution will involve integrating multiple products from multiple vendors into a single solution.

Enterprise mobility is not just about device security or management. Companies need to segment end users by mobility needs; evaluate the types of applications, mobile services and devices to deliver, manage and secure; ensure connectivity and network security are sufficient; and build or improve infrastructure to support their mobility requirements. Organizations also need to consider how to integrate new mobile services into existing IT and corporate services, and deliver mobility in a safe and cost-effective manner.

Traditionally, enterprises looking to manage the influx of BYOD utilize only a small part of the ecosystem solutions, namely mobile device management (MDM) and some level of device security. The scope of what MDM vendors can address in the enterprise mobility ecosystem is relatively limited. Also, not many vendors on the market today can act as a "hub" of solutions and tie together multiple verticals of requirements within the ecosystem. This means enterprises will need to engage multiple vendors, which creates additional layers of complexities that eventually slow down adoption. The best bet for enterprises today is to rely on partners and/or system integrators for mobility implementation, management and operation.
Five Stages of Mobility Maturity

There is no denying that mobility is becoming an integral part of the IT and business strategy. However, it can be quite difficult to gauge what stage of mobile evolution, or maturity, companies are currently going through. Trying to assess the maturity level is further complicated by the different demographics and levels of IT capabilities across the region, from the developed economies of Singapore and Australia to the developing economies of Malaysia and Thailand, as well the industries in which these companies operate.

The mobility maturity model is important for organizations on multiple fronts. First, the maturity model provides a guide for organizations in Asia/Pacific to assess their current enterprise mobility maturity level. Therefore, organizations can take appropriate actions that optimize their progression without making costly mistakes such as implementing overly tactical solutions or solutions they are not ready for.

Second, the maturity model presents a detailed overview of mobility maturity by industry verticals and by country. Organizations can utilize this information to compare their own organization’s mobility maturity to others in the same vertical or compare on a country level, giving the organization a good sense of whether it is ahead or behind the curve in terms of adoption and maturity. This will allow organizations to make better informed decisions on mobility based on their position in the maturity model.

To help enterprises and vendors visualize the levels of mobility maturity, IDC has defined the five key stages of mobility maturity for Asia/Pacific:

Stage 1: Ad Hoc. This first stage is largely experimental, with IT making its first foray into the new world of mobility. Most of these companies would have had previous mobility initiatives that allowed users to access their corporate email through a company issued device. However, this new world of mobility is far more complex as it involves users accessing company information from a multitude of devices and operating systems without the security and control they had in the old single-device model.

The Ad Hoc phase is reactionary, with IT responding to either an initiative from a competitor or succumbing to the demands of employees. The uncontrolled BYOD initiatives that many companies have implemented is a perfect example of this stage, where IT has been pressured to allow employees to use personal devices to access corporate email, networks and applications, but without a proper strategy on how to secure the devices and the applications and content that reside on them. As such, this early stage exposes companies and their IT infrastructure to increased security and potentially regulatory risks.

Deployments in this stage usually target a subset of the workforce and are run as either proof-of-concept projects or pilot programs.
Stage 2: Opportunistic. Stage 2 involves a much more tactical and strategic approach to mobility, where IT begins to define user requirements and the delivery approach is more structured, with proper program management assigned to ensure successful delivery. One of the key differentiators in this stage is that IT will seek to mitigate the security risks created during Stage 1, including defining access rights, securing the transmission of data, and securing the data residing on the device.

During this stage, IT will begin to engage with stakeholders outside of their inner circle to understand their diverse needs and requirements and to regain a bit of the control they lost during the Ad Hoc phase by addressing security vulnerabilities.

The first two stages of mobility maturity most likely will not deliver a positive return on investment (ROI); rather, they will be a cost to the organization. While more mature mobility deployments, such as mobile applications, can deliver an ROI due to the tangible benefits driven from mobilizing business processes, the cost of deploying, managing, securing and supporting mobile devices and users will outweigh the benefits of only mobilizing the person.

Stage 3: Repeatable. During this stage, mobility becomes increasingly strategic as it is accepted by the organization and has the buy-in of key stakeholders, including corporate strategy and the lines of business. These stakeholders will begin to identify horizontal applications that will benefit the business as a whole.

Mobility initiatives will become increasingly complex and capital intensive; however, the benefits will outweigh the costs as successful implementations will deliver a positive ROI. Stakeholders will seek to leverage mobility to drive business value through streamlining business processes, enhancing the customer experience, driving revenue streams and reducing costs.

IT will take a more structured approach to mobile application lifecycle management which will lead to improved application usability and adoption across the organization. However, it will still largely rely on external partners for skills and expertise in developing and launching the more complex mobile solutions.

Stage 4: Managed. This stage is when mobility reaches the level where it begins to drive the business and is used to drive competitive differentiation through the implementation of vertical applications. Stakeholders will collaborate and develop enterprise wide governance of mobility and ensure the mobile strategy is integrated into the line of business and corporate strategy.

IT will begin to invest in mobile infrastructure and platforms in an attempt to build out more flexible and scalable mobility capabilities. In addition, IT will likely create an internal mobile applications development team to rapidly design and develop applications to support the lines of business.

This more structured approach, in which more internal resources are used in the process, will drive ROI and reduce the payback period, providing incentives for
the business to continually expand the mobility offerings and potentially leading to a "mobile first" application development strategy.

Stage 5: Optimized. This is the stage where companies reach mobility nirvana and will leverage mobility solutions to drive and sustain competitive advantage. To accomplish this, companies will seek to mobile-enable not only their employees, but also their suppliers, distributors and customers, effectively mobilizing the channel.

Companies will have deployed an agile end-to-end mobile application lifecycle strategy from requirements gathering, business process re-design strategies, rapid design and deployment capabilities, and robust quality assurance and support procedures.

Mobile development will be integrated into application development teams and mobile will ultimately replace client-side development.

Asia/Pacific Mobility Maturity by Industry

Logic dictates there should be significant variances in mobility maturity levels across industry verticals, as shown in Figure 2, with white-collar industries (e.g., financial services) leading over blue-collar industries (e.g., manufacturing) due to their funding capabilities, regulatory requirements, and robust internal resources. However, IDC research shows that this assumption is not as accurate as it seems. While variances across the verticals do exist, they are not as pronounced as you might believe until you take into account the vertical and country.

FIGURE 2

Mobility Maturity Model by Verticals

A good example of this can be seen when contrasting the maturity levels of the financial services industry in emerging markets, where this industry would be classified as Opportunistic, with the advanced markets (e.g., Singapore, Hong Kong, Australia), where this industry ranks as managed. The financial services industry in
the emerging markets is making strides, with mobile banking initiatives being launched in Thailand as a good example. However, they lack the level of maturity in the advanced markets where it is common for companies to have the following:

- **Mobile Strategy**
  - Well-developed user profiles
  - Defined mobile device and solution roadmaps
  - Moved beyond the “mobility to drive productivity” and leverage mobility to drive competitive differentiation, create new revenue streams and enhance the customer experience

- **Mobile Applications**
  - Multiple applications deployed, including internal (B2E) and consumer (B2C) applications
  - Rapidly accelerating their mobility deployments because of user demand
  - For internal applications, both horizontal and vertical applications

- **Financial and Physical Resources**
  - Allocated mobility budgets
  - Dedicated mobile resources, including development, delivery and support

Another industry that has considerable difference is manufacturing. The advanced markets of Australia, Korea and Singapore are leveraging mobility, in particular around their supply chain to optimize their business efficiency. While still in early phases, this is an area in which companies are investing heavily to streamline processes and workflows. In contrast, manufacturing in the emerging markets is still in the Ad Hoc stage. There are many potential reasons, including a lack of infrastructure and skilled IT workforce, labor intense manufacturing and less development mobility infrastructure and ecosystem, all of which are necessary to design, deliver and support the manufacturing solutions.

**Asia/Pacific Mobility Maturity by Country**

While Figure 3 shows the mobility maturity levels across 11 countries, IDC's research analysis for this white paper will focus on four key markets (Australia, Malaysia, Singapore and Thailand) to illustrate the variances.
The developed markets of Australia and Singapore do come out further advanced than the developing markets of Malaysia and Thailand; however, the results throw out some interesting perspectives.

- **Mobility Strategy**
  - When asked whether their company plans to re-engineer business processes, work flows and roles to leverage mobility, Australia (74%) and Singapore (61%) are at a much more mature phase that Malaysia (40%) and Thailand (28%). This variance is expected as the developed economies have had more experience with mobile solutions and would now be looking to integrate them into their business processes.

- **Mobile Solution Deployment**
  - Two things become clear when looking at the maturity level of mobile solution deployment. First, MDM is much more important in the developed markets, with 70% of Australian and 61% of Singaporean respondents reporting that they will increase MDM spend in the coming 12 months, as compared to only 20% of Malaysian and 10% of Thai respondents. The second factor is that developed countries will continue to drive ahead with their investments in smartphone refreshes and tablet deployments dwarfing the developing countries.

- **Mobile Applications**
  - The developed countries are leading the way in mobile application deployments, platforms and application lifecycle management strategies, illustrated by the fact that 74% of Australian companies are increasing their spend on mobile application deployments compared to only 10% of Thai companies.
Mobility Security

Due to the strict regulatory environments in Australia and Singapore, these countries also lead in mobile security spending. The other contributing factor is that Australia and Singapore are further ahead with mobile application deployments — which come with increased security risks and therefore increasing spend to mitigate those risks would be expected.

Mobile Investment

While Australia and Singapore lead in regard to having defined mobility budgets, the variance is not as large as expected, which is good news for those companies in the developing markets. One possible reason for this is that the developing countries are allocating budgets, but by and large they do not have the budget to increase mobility spend across the board and will therefore focus on targeted areas of spend.

It is important to remember that the mobility maturity level does not coincide with the importance it has with customers in that country. To illustrate, when asked how enterprise mobility ranks in comparison to other ICT initiatives, 42% of Australian respondents said "high" or "very high", followed by Thailand (32%), Singapore (28%) and Malaysia (21%). While Thailand might not stack up to the more developed countries in terms of mobility maturity, it does so in terms of enterprise mobility focus within the enterprise.

ESSENTIAL GUIDANCE

Enterprise Mobility Framework

As companies embark on their mobility journey, they typically start off at Phase 1 (refer to Figure 4). The initial implementations tend to be in response to either user demand or competitors' moves and are not undertaken with a proper mobility strategy or consideration for the security risks. This reactive approach has contributed to the overwhelmingly low satisfaction levels, with only 24% of companies surveyed (source: IDC's Future Workspace Survey, May 2013) satisfied with their current mobile deployments. In addition, this lack of strategy also leads enterprises to invest in point solutions that meet an immediate requirement rather than providing a platform for growth. Like many things in life, the simple solution that provides immediate benefit is not the best approach. IDC recommends that companies take a step back to Phase 0 to define their mobility objectives and identify the path to achieve their goals.
Phase 0. Define the Mobility Strategy. Before implementing enterprise mobility solutions, organizations should ensure a well-defined strategy is in place and potential security risks are addressed. Strategically, enterprises need to understand their unique user profiles and design device and solution roadmaps that will deliver tangible business benefits to their individual environments. As for security, enterprises will need to approach it holistically by addressing key aspects previously discussed.

Phase 1. Mobilizing the Person. Mobilizing the person involves deploying solutions that enable the anywhere, anytime and on any device access that the users require, in a secure manner. Whether companies issue a single device to all employees, leverage a CYOD model, or launch a BYOD initiative, the objective is the same – giving users basic access no matter where they are or what device they are using. When done properly, this phase lays the foundation on which the latter phases will be built. However, more often than not, companies languish in this phase with no strategy on how to move onto the next phase – mobilizing the process.

On the surface, this might not seem like that big of an issue. However, companies will soon realize this phase does not deliver the tangible business benefits to support the costs of supporting it. If a company effectively mobilizes their people, they will have to fund additional costs, including providing device management costs to fund an MDM solution to manage their devices; security costs to mitigate their increased risks; support costs to manage the devices, solutions and users; and increased bandwidth costs if they allow for unmonitored BYOD access to their network.

Phase 2. Mobilizing the Process. Mobilizing the process happens once the underlying foundation for enterprise mobility has been established. Mobilizing the process involves taking existing business processes and optimizing them for mobile devices. For example, sales can use mobile-optimized customer
relationship management (CRM) applications to log client interaction with their smartphones or tablets, which increases productivity and efficiency and should correlate to increased sales.

The challenges of mobilizing the process are twofold. First, when a company seeks to mobilize a business process, additional stakeholders will be involved. In addition to IT, they must involve the lines of business, end users, finance, strategy and HR just to name but a few. In Phase 1, mobilizing the person, IT can make decisions on their own. But when seeking to change a business critical workflow or business process, increasing stakeholder involvement is a must.

Second, mobilizing the business process can be a more complex technical challenge. It will require procuring additional software solutions or reengineering existing solutions, or sometimes both. Decisions must be made regarding the viability of mobilizing legacy systems versus investing in new enterprise software solutions and whether those new solutions should be managed internally or hosted. The potential impact on existing IT infrastructure must not be underestimated due to the potential impact to business processes and customer support and management.

Phase 3. Mobilizing the Channel. Mobilizing the channel involves collaboration between the organization and its value chain partners. This is very much like Phase 2, but the organizational and technical complexities are much higher due to the number of participants, which could include suppliers, distributors, and hosting partners. However, the payback of mobilizing the channel can also be tremendous if properly designed and implemented and could lead to significant competitive advantage. Mobilizing the channel can streamline the entire value chain operation, allow quicker time to market, and resolve issues before they become problems.

IDC believes that channel mobilization can be accomplished in any industry vertical. However, some verticals, such as manufacturing or logistics would have an easier time mobilizing their channels than verticals that have a more ambiguous or restrictive channel structure, such as education and government. Nevertheless, mobilizing the channel is possible in less channel-defined verticals so long as organizations approach it on a partner-by-partner basis, and work with partners that can deliver the highest ROI by going mobile.

CONCLUSION

The journey to fully capitalize on the opportunities afforded by enterprise mobility is long and challenging. Unlike so many other enterprise ICT innovations, mobility is not being driven by IT at the moment. Such revelations may be difficult for IT managers to acknowledge, but acceptance will set the right mindset for organizations to regain the control that IT has lost. Despite the chaotic mobile device marketplace and confusing selection of security and management solutions, clarity can be found if the organization approaches mobility holistically.
Given the nascent nature of enterprise mobility in the Asia/Pacific region, organizations are expected to engage its channel partners during multiple phases of the mobility project. While partners can provide the expertise needed to deliver multivendor mobile solutions, companies themselves are responsible for aligning technology with strategy. This means organizations need to deepen their understanding of mobility internally in order to select the best solutions that address the mobility needs of the company, both technically and strategically.

Finally, the rise of consumerization is a wakeup call for IT departments across Asia/Pacific. At the same time, enterprise mobility offers IT a chance to regain some of the relevancy it has lost with the users. IT can no longer survive as an organization that simply "keeps the lights on", but rather one that facilitates the corporate transformation in a mobile-centric era. As the enterprise mobility market continues to consolidate, more vendors and partners can deliver multifaceted solutions, but IT must evolve into a more strategically significant organization in order for enterprise mobility to deliver any measureable value to the enterprise.

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2013 IDC. Reproduction without written permission is completely forbidden.