Mobility

The Next Wave

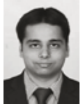
Nitin Khanapurkar, N. Subramanian, Nikhil Kulkarni, Zubin Mehta and Shadab Wadiwala

N. Khanapurkar
is partner with Management Consulting at KPMG in the UAE.
nitinkhanapurkar@kpmg.com

N. Subramanian
is technical director with Management Consulting at KPMG in Mumbai, India.
subramanian@kpmg.com

N. Kulkarni
is manager at KPMG in India.
nkulkarni@kpmg.com

Z. Mehta
is assistant manager at KPMG in India.
zubin@kpmg.com



Sh. Wadiwala
is consultant with IT Advisory practice at KPMG in India.
shadabwadiwala@kpmg.com

Enterprise Mobility is not simply another trend for IT departments to support with a shrunken form factor or a new category of enterprise applications. Rather, enterprise mobility manifests a broader shift to new systems of engagement and is heralding many disruptive technology and business model innovations in enterprises today. The need is for CXOs to understand this phenomenon in its entirety and empower customers, partners, and employees, while at the same time keeping the risks of adopting this disruptive force at bay.

Introduction

In the past two decades, the mobile phone has evolved from an audio device capable of merely making and receiving calls to a powerful device used for internet banking, movies, games, social media and even a go-to device in times of emergencies. Mobile phones today are substitutes for newspapers, desktop computers, gaming consoles and even travel tickets. Movies and television episodes are being streamed online. Tweets, instant messages, and hangouts are everyday conversation techniques.

In business, mobile devices have evolved from merely providing ubiquitous access to enterprise email (read: Blackberry™), to enabling business through salesforce automation and customer feedback / sourcing apps that have the potential to change business models for good. Early movers are already arming their sales force with tablets, setting up enterprise app stores as well as enabling and adopting employee-friendly policies such as BYOD. But is mobility adoption only about embracing new technologies, bringing in a new set of vendors or devices into the IT ecosystem? Sure it's cool and keeps enterprises popular with employees and customers alike, but what is the value mobility brings, and how does it stack up against the risks that it exposes business to? And how do businesses weather the mobility related challenges?

With the entry of the millennial in the workforce, employees have come to expect not just ubiquitous access but also access from any device, including personal devices; "Why can't I use my own? I love my phone" is a common question which brings even the most robust and efficient IT processes to a standstill. A foreign device in the enterprise environment is a nightmare for the IT manager and more so for the Information Security manager.

Mobility is also spreading beyond social applications, reaching products extending fundamental business functions of Business Intelligence and Analytics (BIA), Customer Relationship Management (CRM), Knowledge Management Systems (KMS) and employee service portals. Similarly, when using mobile for customer service and customer outreach applications, there are twin challenges of protecting and securing access to enterprise information assets and protecting customer data privacy and confidentiality.

Businesses worldwide want to leverage mobility-based solutions to enhance business productivity, visibility and flexibility. There is an increasing trend to allow employees to use their personal mobile/tablet devices at work for accessing corporate apps and email. Bring Your Own Device (BYOD) is making rapid entry into the business world, with demand arising through groundswell from employees rather than top-down IT strategy decisions.

There are mechanisms that can help businesses provide environments where employees can connect their personal devices to an enterprise network while keeping the

It is imperative that security design is incorporated in each step of the mobile app development lifecycle

security challenges at bay. A combination of appropriate policy initiatives synchronized with implementation of technology solutions can help businesses overcome all the challenges of enterprise mobility.

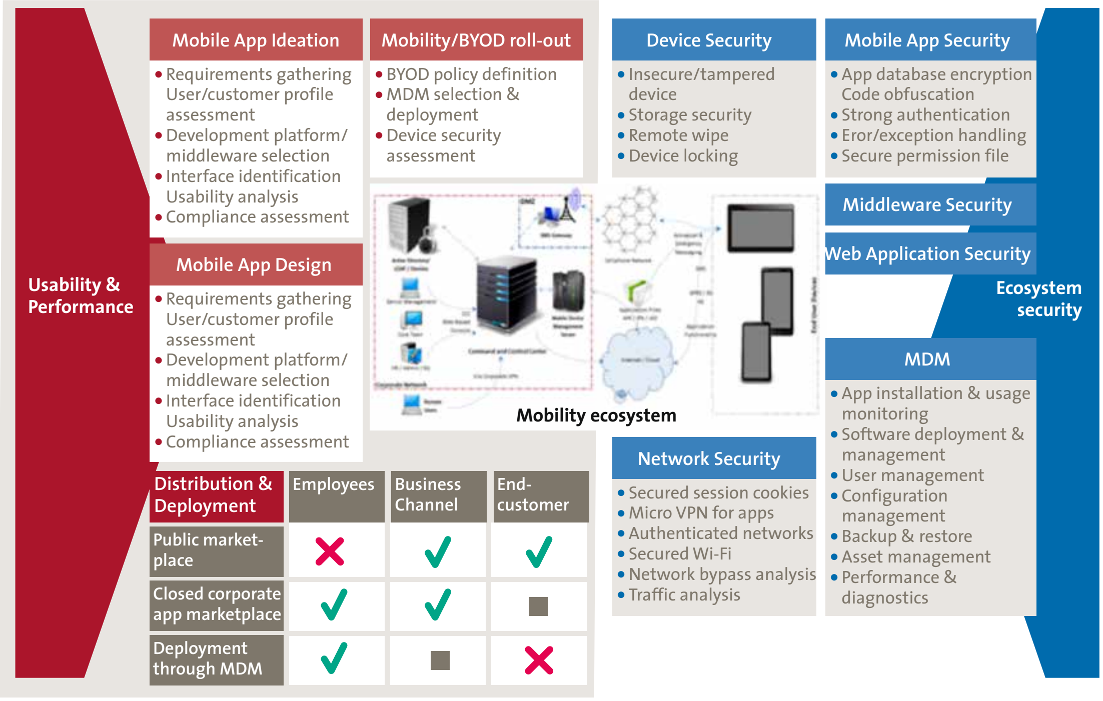
Challenges of Enterprise Mobility

Application Security

Mobile apps have emerged as the primary interface for delivering mobile solutions to consumers, partners and employees. Apps enable rich, task-oriented functionality and user experience that mobile consumers demand. This makes it imperative to incorporate security design in each step of the mobile app development lifecycle. Businesses often outsource mobile app development, while some also have in-house capabilities for app development. In any case, the rapidly changing world of mobile platforms results in challenges to keep the development team updated with the latest security threats and prevention strategies. At the same time, the app remains the heart of mobile security and needs to have security considerations, irrespective of the other security mechanisms employed within the ecosystem.

Mobile apps need to be secured against vulnerability arising from accepting invalid input values. For example, corrupt user input, especially in form of file uploads, may result in remote execution of the code cascading into unauthorized access and loss of confidential data. Another example is the inability of apps to detect rooted or jailbroken devices, leading to risk of multiple exploits, such as privilege escalation, further resulting in breaches of confidentiality and data integrity. Similar challenges involve preventing apps from running on emulators and insecure logging/caching mechanisms, which might increase risks of data leakage. Native mobile OS and device vulnerabilities also present unique security concerns like kernel exploits and firmware bugs that app developers need to be aware of and consider during app development.

One of the new technologies on the drawing board is Near Field Communication (NFC), which allows people to share business cards and URLs when in close proximity. NFC is also used to make mobile payments at point-of-sale (POS) terminals. However, a principal research consultant at Accuvant Labs has found serious vulnerabilities around


Usability & Performance
Mobile App Ideation
• Requirements gathering User/customer profile assessment
• Development platform/ middleware selection
• Interface identification Usability analysis
• Compliance assessment
Mobility/BYOD roll-out
• BYOD policy definition
• MDM selection & deployment
• Device security assessment
Mobile App Design
• Requirements gathering User/customer profile assessment
• Development platform/ middleware selection
• Interface identification Usability analysis
• Compliance assessment
Mobility ecosystem
Device Security
• Insecure/tampered device
• Storage security
• Remote wipe
• Device locking
Mobile App Security
• App database encryption Code obfuscation
• Strong authentication
• Eror/exception handling
• Secure permission file
Middleware Security
Web Application Security
Ecosystem security
MDM
• App installation & usage monitoring
• Software deployment & management
• User management
• Configuration management
• Backup & restore
• Asset management
• Performance & diagnostics
Network Security
• Secured session cookies
• Micro VPN for apps
• Authenticated networks
• Secured Wi-Fi
• Network bypass analysis
• Traffic analysis

Distribution & Deployment	Employees	Business Channel	End-customer
Public marketplace	✗	✓	✓
Closed corporate app marketplace	✓	✓	■
Deployment through MDM	✓	■	✗

Figure 1. **Mobility ecosystem.**

NFC that can launch attacks on a victim's device, resulting into making automated phone calls, sending SMSes and accessing personal data such as contact lists[1].

While some vulnerabilities in mobile apps can be detected through a Vulnerability Assessment exercise, and many can be addressed by adopting secure coding practices, often security enhancements within the mobile app alone may not be sufficient. It is necessary to adopt a holistic approach encompassing security testing of the entire mobile ecosystem, comprising enterprise app stores, web services, web applications, native mobile device platforms and any intermediate platforms such as IDEs, code libraries and even Mobile Device Management (MDM) systems.

Application functionality

App permissions are another important consideration from the perspective of app security, albeit users might just accept the default permissions without much thought. On Android, every app prompts the user to accept the permissions that are required for functioning. However, users may not always understand why a specific permission is required by an app. In a world where even your teenage neighbor can develop a mobile app and launch it on the App store, it is important to understand the difference between a valid permission and a suspicious request. For example – Does that gaming app need to track your location? Does it need to have internet access? Does it need to have the ability to make calls or send messages? Do you want to allow it to take photos? There are several apps on app stores that want the ability to make calls, send messages or read contacts on a user's behalf – one needs to critically question if all of them indeed need such permissions, especially given that theft of email addresses, phone and credit card numbers is a serious concern.

Apps may not always inform users about the personal data they collect, how and where this personal data is stored and if it is destroyed upon deactivation or un-installation of the app. As revealed on Wired.com, the virtual assistant app Siri retains a record of all the things you ask it for six months on its servers[2]. Most of us concern ourselves with the repercussions of such private information being misused by marketers to spam us, but if the data being stored concerns private records, such as credit card numbers or health data, the repercussion of loss of such data could be as serious as financial loss or identity theft. According to a recent study conducted by Appthority, a company specializing in mobile app risk management, the top 50 free iOS and Android apps access a user's contact lists, calendar data, track a user's location, send unencrypted data and share data with ad networks[3]. Appthority tested apps in the business, education, entertainment, gaming and finance categories. Among these, entertainment apps were the worst when it came to user privacy. This category had the highest number of apps that tracked location and shared data with ad networks.

Device Theft

Device theft is another real cause of concern. Millions of mobile phones are stolen each year globally. According to research done by Kensington, every year around 70 million smartphones are lost and only 7% of them are recovered[4]. When devices are lost or stolen, all the data stored on the devices may be compromised, if sufficient device protection in form of power-on passwords is not added. If users are not consciously aware about security risks presented by mobile apps, they may, for the sake of convenience, not password-protect their device. If they also don't fully log out of social media apps, this might result in misuse of personal data. Device theft assumes greater significance given that employees also access corporate emails through mobile phones, and as individuals we access social networks, engage in online shopping and even handle financial affairs using mobiles. According to Kensington research, about 60% of stolen smartphones contain sensitive data in the form of contact lists, emails, internet credentials, business apps and mobile payments information. Hence mobile device theft remains a great concern for business.

Third-party App Store

App distribution is also an important aspect of the mobile ecosystem. Google Play and Apple iTunes are not the only distribution channels of mobile apps today. Apart from native OS app stores, many third-party independent mobile app stores have emerged. Such app stores can look attractive to the naive user, as they often distribute pirated

» Does that gaming app need to track your location?
» Does it need to have internet access?
» Does it need to have the ability to make calls or send messages?
» Do you want to allow it to take photos?

[1] http://www.digitalnewsasia.com/hack-in-the-box/to-nfc-or-not-to-nfc

[2] http://www.wired.com/wiredenterprise/2013/04/siri-privacy/

[3] Appthority 2013 report

[4] http://blog.kensington.com/wp-content/ktg/docs/m1_iphone_theft_banner.pdf

versions of mobile apps that are available for a fee on official app stores. An investigation led by Techweb.com, a Chinese news website, has found that there are numerous third-party or unofficial app stores that lack basic quality and security checks on the apps they distribute[5]. Users therefore face a potential risk in downloading pirated apps from such sources, which are apparently legitimate but are often infected with malicious data-stealing code.

The security policies of different app stores vary, and a majority of third-party app stores have little or no approval process in place with no concern for user security. Since smartphones often carry more personal data than laptops, usage of unauthorized apps may result in theft of personal data such as contacts, email addresses etc. Stealing credit card numbers can also lead to financial losses, as can unintended auto-subscribing to paid VAS services through the app.

However, not all third-party app stores are clandestine in nature. Many third-party app stores are operated by local mobile network operators or device manufacturers, which offer tailored content considered safe. [6]For example, the Amazon app store follows a code-review-based approval process to vet all apps before distribution on their app stores, a process similar to the one followed by the official Apple app store.

Enterprise App Stores

Listing business apps on a public app store such as Apple iTunes or Google Play not only requires the business to modify the app to suit the store's own policy, but also creates potential challenges for IT departments in terms of security and governance. At the same time, due to widespread adoption of mobility within business, many corporate users now want the same convenience and ease of use at the workplace that the online app stores offer. A potential solution to this is the business's own private enterprise app store (EAP) that provides a user-friendly self-service experience commonly found on consumer app stores but at the same time allows the business to manage access controls and compliance as per their internal policies. However there are a few challenges in successfully implementing and operating mobile app stores in the enterprise ecosystem. These challenges revolve around:

- Supporting multiple mobile OS platforms and abrupt changes in mobile space in order to ensure a synergy with BYOD program.
- Selecting the right suite of mobile apps to be featured on the app store. Post deployment maintenance, such as regular introduction of fresh, industry-tailored content.
- Promoting and displaying applications as recommendations to the enterprise app store user.
- Integrating licensing mechanisms within app stores and understanding infrastructure costs.
- Access control on apps distribution and pushing upgrades on a diverse range of mobile platforms.
- Handling integrations with corporate resources, such as identity management systems, in order to implement single sign on (SSO).
- Implementing dashboards for better visibility into app subscriptions, usage, license audits and policy compliance.
- Interfacing of enterprise app stores with mobile device management (MDM) software.
- Creating branded app stores targeting a specific enterprise user group, such as HR, Call-center, Sales force etc.

According to Gartner, 25% of businesses s are expected to have their own enterprise app stores by 2017[7]. Thus with the growing reliance of companies on mobile devices and apps, enterprise app stores accessible only to employees of an organization are on the rise. At the same time, it is essential to handle the above challenges for successful adoption of mobility within the enterprise.

Enterprise Mobility Enablement

One of the key aspects of successful implementation of an enterprise mobile strategy is selecting the appropriate mobility solution that is aligned with the organizational goals.

With several organizations deciding to support both corporate-issued and employee-owned devices, it is also equally important for them to establish new governance policies as well as ways to manage and secure these new mobile technologies and their corporate data. Enterprises need to consider several important factors when choosing enterprise mobility solutions.

Listing a manufacturer's apps on a public app store requires the manufacturer to modify the app to suit the store's policy.

[5] http://www.techweb.com.cn/internet/2011-10-27/1110939.shtml – Article in Chinese

[6] https://developer.amazon.com/help/faq.html

[7] http://www.gartner.com/newsroom/id/2334015

Automated solutions also need to be augmented with appropriate security policies and device settings.

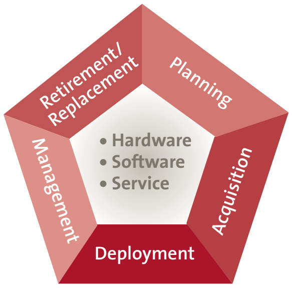


Figure 2. **Mobile Device Management Source: KPMG in India Analysis.**

Mobile Device Management (MDM)

The essential first step in providing a secure BYOD program is setting up a mobile device management (MDM) solution: specialized software intended to distribute mobile applications, define device configuration settings and implement IT Governance policies on mobile devices irrespective of the ownership[8]. An MDM solution can be employed to control enterprise-owned and employee-owned (BYOD) devices, and also mobile devices owned by channel partners and even clients. MDM's provide real-time management capabilities including enforcement of corporate IT policies, self-service and optimized security of mobile communications, while minimizing cost and downtime. Selecting a MDM system is often the first step businesses take towards implementing a secure BYOD. MDM provides the IT administrator with the ability to enforce security settings in the end-user devices such as password strength and policy, email, VPN and Wi-Fi, power-on-password etc. MDM also allows the ability to remotely install/uninstall the mobile apps on the device with the capability to provide software updates and mobile OS patch management. Mature MDM solutions also provide asset management and the ability to detect and deactivate jail-broken/rooted and non-compliant devices from the enterprise network.

With the ability to perform remote and selective data wiping, MDM solutions form a backbone of secured application distribution and device management. These functions can be performed under various scenarios, including device theft and uninstalling of enterprise apps. MDM enables remote wipe of the data. MDM also helps in enforcing encryption and compartmentalization of enterprise data residing on the mobile device. Today MDM solutions offer both Software-as-a-Service (SaaS) and on-premise models. MDM does provide employees with access to the enterprise application using the device of their choice without compromising security measures.

Secure coding

Whilst MDM assists in secure distribution of apps and management of devices, mobile applications themselves also need to adhere to the security norms of the enterprise and best practices followed in the industry. Developers must define and enforce a baseline of security standards across the mobile solutions they develop. Security needs to be built in the mobile app code and the architecture itself.

Some of the primary secure app coding techniques to ensure app security are:

- Using code obfuscation techniques to disguise the app logic
- Disabling copy-paste functions for critical input fields like passwords, PINs, usernames, payments etc.
- Strong encryption for data transfer, especially for apps dealing with financial or otherwise private and confidential data
- Data leakage needs to be avoided using session control, secure logging and clearing residual memory heaps on exit
- Performing client as well as server-side input validations
- Some other secure measures include disabling screen capture function, preventing apps from working while connected to unsecured Wi-Fi networks, using SIM / device ID authentication and configuring appropriate session timeouts for critical financial apps such as mobile banking
- For advanced security, app containerization techniques need to be implemented in order to have better control for avoiding memory and data leakage issues.

Micro VPNs

If MDM forms the backbone of secured enterprise mobility, and secure app development forms the baseline for the application development, a secure connection would complete the trio to secure the transfer of data from and to the app. Increasing use of mobiles and tablets to remotely access corporate LAN has also introduced a strong need to use secure VPN connections on mobile devices as well. The traditional VPN connection sets up a tunnel between the device and a gateway through which all traffic must flow. However, the limitation of such a VPN connection is that it is not possible to compartmentalize personal and corporate traffic and allow only corporate traffic to use the tunnel while allowing non-corporate traffic to use the open connection. In addition, it is not possible to allow only selected apps to use the VPN tunnel, or to require the device in its completeness to be bound to the enterprise's BYOD policy (sometimes enforced from an MDM).

However, with advancement in technology it is now possible to create on-demand application-aware VPNs, known as "micro VPNs." Micro-VPN tunnel is established on a need basis when the user invokes the app that requires corporate network access. Unlike traditional VPN tunnels, which get disrupted, micro VPN seamlessly handles gaps in network

[8] Making Emerging Technologies a Boardroom Agenda

Enterprise Mobility is not a product to purchase or a policy to put in place; it's a process that starts with aligning the mobility initiative's strategic goals with that of the organization.

coverage, roaming networks, suspend/resume of mobile devices and, at the same time, provides an encrypted channel to transmit data from specific apps without binding the complete device traffic to the VPN tunnel.

Mobile AntiVirus/Security apps

Device security is also an important aspect along with the above methods. Mobile security apps have emerged to offer proactive protection against malware, viruses, and spam and phishing attacks. Some security apps also encompass a firewall security offering real-time protection. Some of the advanced security apps also offer secure web browsing and anti-theft components, such as being able to activate GPS on your phone to track down its location in case of theft. Mature security applications even offer advanced features such as remote locking and resetting of the device to factory defaults via preset messages sent from pre-selected mobile numbers to the stolen device. In case the resident SIM card is removed; anti-theft applications also prevent the disabling of data and location-tracking services, and would send the GPS coordinates of the new SIM card to the owner of the device. The GPS coordinates then can be tracked to locate the stolen device. These security apps are offered as free and paid versions. While free versions offer basic features like scheduled scans, paid versions provide advanced functions such as enabling remote locking of the phone to protect information, and scanning apps to provide details on any suspected spurious activity by apps.

Settings versus Policies

Finally, automated solutions also need to be augmented with appropriate security policies and device settings. The latest versions of mobile operating systems provide native support for many security features such as remote data wiping, digital certificate, storage security, permissions enforcement, etc[9]. IT departments need to keep their knowledge bases updated in order to effectively exploit these features and balance security with accessibility.

Further, organizational policies and procedures provide a foundation for the implementation and enforcement of security features. Some common aspects that need to be considered for a secured mobile computing environment are:

- Implementing whitelists and blacklists for permissible apps
- Disabling installation of apps from third-party and unofficial app stores
- Enforcing device-level storage encryption
- Remote data wiping upon SIM change, device theft, etc.
- Enforcing screen lockout time with unlocking passwords.
- Disable connections to unsecured Wi-Fi networks.
- Micro VPNs for accessing corporate content
- Jailbreak/rooting detection in order to ensure compliance with enterprise mobile security policies

While MDM solutions can automate the delivery and configuration of settings to the device, one cannot rule out the role played by the device's resident security settings, which are often controlled locally by the users themselves. Some common security settings that users can set at their end are:-

- Disabling NFC, Bluetooth and Wi-Fi when not required
- Implementing SIM lock PINs
- Password protect paid-apps purchases
- Enforcing power-on PINs
- Disabling GPS when location information is not required
- Making passwords invisible

To recap, Enterprise Mobility is not a product to purchase or a policy to put in place; it's a process that starts with aligning the mobility initiative's strategic goals with that of the organization, selection of the ecosystem partners, application development management and IT risk and security that must be performed on an ongoing basis. It is also critical for an organization to continuously balance the risks and benefits in its business environment and even outside. Organizations need to systematically integrate protection into the way they operate and implement Enterprise Mobility.

[9] http://developer.android.com/about/versions/kitkat.html

Conclusion

Enterprise IT has always been a two-headed monster – on one hand, the accelerated emergence of new technologies has heralded new business models; on the other hand, resulting risks have to be tamed through laborious and disciplined risk management. Enterprise Mobility is no different – however, with its proliferation outside the enterprise to customers and beyond, the risks it exposes are far more widespread and consequently even more difficult to manage.

In addition, businesses that adopt the stance of "don't adopt and don't manage" with mobility face impending obsolescence. Not addressing the challenges to mobility is not an option, as it will inevitably hamper the business in its use of mobility and might result in reputational loss and, in some cases, even a direct loss of business.

Whether the business is a technology provider itself or a pure brick-and-mortar undertaking, mobility enablement will require a combination of top-down and bottom-up approaches. Defining appropriate policies and guidelines needs to be complimented by deployment of technology solutions such as MDMs and enterprise app stores. At the other end, employee awareness and training, coupled with stringent security assessment of enterprise mobile apps can provide much-needed comfort to the IT management from the nightmares of losing control over the security of enterprise data and systems.

About the authors

N. Khanapurkar is partner with Management Consulting at KPMG in the UAE, and has over 22 years of work experience, spanning 4 continents, in the field of Business, IT and Risk Consulting. His earlier experience has been with leading organizations including Deloitte and Andersen. His areas of focus include Business Transformation through emerging technologies like Cloud Computing. He is a well-known speaker and has authored several publications on the subjects of Cloud Computing, BCM and Physical Security.

N. Subramanian is technical director with Management Consulting at KPMG in Mumbai, India. His total professional background spans four continents and over 22 years of work experience in the field of IT Management Consulting, Risk Consulting, Auditing, and Implementation of ERP/business solutions. The clients he has worked with span various sectors from Consumer Markets to Telecom to IT /ITeS companies. Subramanian has worked with organizations to guide them in evaluating business solutions and creating a road map. His main focus areas include Information Security, Technology Audits and Business Continuity Management.

N. Kulkarni is manager at KPMG in India. Nikhil has close to 9 years of experience in advising clients in the areas of IT Transformation, IT Architecture, Project Management, IT Governance and Sourcing. Nikhil has a keen interest in exploring the application of emerging technologies to the business environment. Nikhil has worked with clients across the Financial Services, IT/ ITeS and Telecom sectors and has been a involved in multiple Thought Leadership publications relating to the Cloud, mobility, and technology transformation in the Media Industry and mobility.

Z. Mehta is assistant manager at KPMG in India. He has over 14 years of work experience in consulting, outsourcing, IT/ITeS & media sectors spanning 2 continents. A member of the core team for Global Technology Incubator (GTI) for Cloud Computing within KPMG, he has contributed to thought leadership on the media sector, emerging trends and cloud computing. Zubin has worked with clients across the media, IT, Telecom and Financial services sectors and currently focuses on Cloud Computing, Social Media and Enterprise Mobility. Prior to KPMG, Zubin has also worked on projects with leading global telecom and technology providers in areas of process migrations, operations transitions & process re-engineering, response and contact center management and Business Continuity Management (BCM).

Sh. Wadiwala is consultant with IT Advisory practice at KPMG in India. He has worked across a wide array of computer technologies such as Java Programming, Virtualization, Cloud computing, Enterprise Mobility and Network security. He was also a member of Global Technology Incubator group for Cloud Computing within KPMG. Currently his focus areas are Cloud computing, Social Media and Enterprise Mobility. Shadab is also involved in the ideation of Mobile apps and MDM vendor evaluations. He also contributes to KPMG thought leadership on emerging trends such as BYOD, Enterprise Mobility and Bid Data.