ON OUR RADAR

THE CHALLENGES OF ENTERPRISE MOBILITY

By Jay Emmanuel

Welcome to the Summer 2012 issue of the *IQT Quarterly.* With a special focus around the challenges of enterprise mobility, this issue builds on topics discussed in our Winter 2011 edition, "Moving to Mobile: Trends, Technology, and Solutions." Since the publication of that issue, IQT has continued to collaborate with our Intelligence Community partners to brainstorm architectures and designs for secure and scalable enterprise mobile rollouts. This has been a tremendous learning experience for IQT as we cultivate our understanding of the IC's requirements and track trends in the rapidly evolving commercial market. These discussions have allowed us to focus on companies and technologies that address current government challenges.

Mobility for the enterprise is an inevitable phenomenon that will continue to grow over the next few years. The Blackberry-centered mobile framework provided a one stop, locked down solution for IT organizations that was easy to adopt and use. With RIM fast imploding and with the tremendous consumer uptake of Android and iOS devices, the mobile IT environment has become far more diverse and challenging in terms of devices, operating systems, security risks, and other issues that are commonly of concern to organizations. Users within the enterprise now demand a mobile experience that is on par with or better than commercial applications. This new mobile world is redefining the function of traditional IT in the workplace and presents organizations with a set of complex security, management, cost, compliance, and legal issues that need to be addressed.

Security

Mobile devices provide a much larger and more diverse attack surface for an adversary. With the growing trend of Bring Your Own Device (BYOD) policies in organizations, these risks are further elevated. A lost or stolen employee-owned device with permanent VPN connections for email and other applications can provide easy access into the enterprise network where corporate data and sensitive information are stored. Techniques like device locking, data-at-rest encryption, enterprise- and application-level sandboxing, device virtualization, and secure boot loaders that mitigate corporate risk are all evolving in the commercial world. Mobile Device Management (MDM) and Mobile Application Management (MAM) are relatively mature and help with risk mitigation — it is not expensive or difficult to get robust and scalable tools that are designed for this next generation of mobile IT.

Policy and Compliance

Establishing and adhering to an organization-wide policy for mobile devices is a key step towards the effective management of enterprise technology. Questions like whether or not to allow BYOD, how to effectively sandbox user and personal data, how much to lock down an enterprise device, whether or not to allow split tunneling of user traffic, and whether to route all uplink and downlink traffic through enterprise infrastructure need to be addressed at both a corporate and department level since all have ramifications at various levels within the organization. Once organizational policies are defined clearly, employee education and enforcement of the policy on the device and network are necessary. Plans for immediate and effective remediation should be implemented in the event a policy is violated.

Usability

Consumers have grown to expect a user experience from enterprise applications that matches or exceeds that provided by commercial applications. A clunky enterprise app or a device that is considered too locked down isn't likely to be widely adopted, and users will find ways around policy that is deemed to be too restrictive. Optimizing usability requires that the enterprise create commercial quality apps without compromising the security posture of the device or the network. Consumers are comfortable downloading apps from an app store; creating a similar experience in the enterprise will likely increase enterprise application use and adoption. Users should also be confident that they are free to use their devices for personal use with the assurance that there will be a clear separation between personal and enterprise content.

Enterprise Applications

Enterprise mobile applications need to effectively extend backend IT services and present enterprise data to a mobile device quickly and easily. Integration between the mobile device and backend systems should be a seamless and effective process both for an enterprise app developer and the end user. For the developer, implementing security policies and access to backend services like authentication, directory, and authorization services should be a transparent process that is easily incorporated using standard libraries and APIs. Given the wide array of devices and operating systems that the application needs to work on, solutions that allow web developers with traditional programming skills to create device and operating system agnostic mobile applications will be critical in achieving application development scale.

Rapid Rate of Change

Designing a scalable and secure mobile enterprise architecture is complex, especially given the fact that the technology platforms and devices are evolving at a fast pace. Most IT organizations are accustomed to a Microsoft-like 5-6 year product lifecycle in which they have the time to plan changes and slowly implement them. Mobile evolves very fast from every perspective — devices, versions of operating systems, diversity of available applications, and the types of security threats on these devices are constantly changing. A well thought-out and successful mobile strategy will plan for change and select architectures that allow for future adaptation to emerging trends.

Cost Management

A mobile device's cost continues long after initial deployment and is often challenging to determine and manage. Besides the capital costs associated with the devices, usage rates are only increasing with the proliferation of bandwidth-hungry applications. With BYOD, enterprise users present the organization with a wide array of bills and user-purchased service agreements. Cost visibility in real time is essential to defining and maintaining expense policies. International roaming charges can have a serious impact on costs and have been the focus of many recent cost-related mobile decisions. Most Mobile Device Management suites provide real-time cost visibility. Targeted analytics that yield insight into usage patterns in relation to business operations and geographies can help with understanding costs.

These are but a few of the many challenges that are associated with mobile IT. IQT will continue to engage with cutting-edge companies in this space to stay abreast of technology trends. While this is sometimes a daunting task since this is a relatively new and emerging area of technology, it remains exciting and challenging to us as we help guide customers on strategies in the mobile space. Q

Jay Emmanuel *serves as Vice President in IQT's Information and Communication Technologies Practice. Prior to joining IQT, he worked extensively in the mobile space with Motorola, Hughes Network Systems, and most recently with Megisto Systems, a startup that developed carrier-grade mobile gateways. Jay has a Master of Science in Computer Engineering from the University of Maryland at College Park.*