IQT
QUARTERLY
VOL. 7 NO. 1 SUMMER 2015

PLANET OF THE APPS

Advances in Enterprise Mobile Applications

IQT
IN·Q·TEL

IQT Quarterly is a publication of In-Q-Tel, Inc., the strategic investment firm that serves as a bridge between the U.S. Intelligence Community and venture-backed startup firms on the leading edge of technological innovation. *IQT Quarterly* advances the situational awareness component of the IQT mission, serving as a platform to debut, discuss, and debate issues of innovation in the areas of overlap between commercial potential and U.S. Intelligence Community needs. For comments or questions regarding IQT or this document, please visit www.iqt.org, write to iqtquarterly@iqt.org, or call 703-248-3000. The views expressed are those of the authors in their personal capacities and do not necessarily reflect the opinion of IQT, their employers, or the Government.

IQT
QUARTERLY

Identify. Adapt. Deliver.

TABLE OF CONTENTS

ON OUR RADAR

Mobile Apps are Eating the World

By Isaac Myauo

In late 2014, Benedict Evans of Andreessen Horowitz presented "Mobile is Eating the World," where he provided insights on how mobile technology is redefining the Internet and broader tech industry. Evans cited statistics on how users spend more time using mobile apps than the rest of the Web, how mobile first transforms development and capital requirements, and how mobile technology creates new business opportunities that are the foundation of industry disruption. We saw tremendous growth in mobile in 2014, but the enterprise still faces many challenges. This issue of the *IQT Quarterly* builds on topics discussed in our summer 2012 edition, "Slide to Unlock: The Challenges of Enterprise Mobility" and focuses on the challenges the enterprise faces after issuing or allowing mobile devices.

Mobile technology is a phenomenon that has evolved over the last few years and is continuously transforming the consumer market. In the enterprise, 2014 saw an increased focus on mobility and the importance of apps for business. The partnership announced between Apple and IBM to transform enterprise mobility seeks for IT organizations to first easily adopt, use, and support mobile platforms, and secondly demonstrate the importance of well integrated enterprise apps. Google's announcement and recent release of Android for Work provides increased management and data separation for work-approved apps. While corporations have largely adopted mobile device management (MDM) solutions to secure, manage, and control the device, the mobile operating system (OS) industry has also seen a greater need and push to focus on security and privacy beyond the device in response to the challenges within the mobile IT environment.

The rapid adoption of mobile devices and mobile apps by consumers has translated to the enterprise. Users within the enterprise now demand a mobile experience that is on par with or better than commercial apps. This presents app developers and IT organizations with a set of complex issues surrounding security, management, development, time-to-market, cost, performance, and user experience that need to be addressed.

Security

Securing mobile apps is a challenge — breaches and data leaks can be disasters. Bring Your Own Device (BYOD) policies elevate this risk for the enterprise. Enterprise mobility management (EMM) solutions have evolved and are relatively mature in mitigating risks by providing scalable tools to manage the device, force encryption, sandbox apps, and set policies, but IT departments have lost the degree of control in decision-making they once had regarding device approval. The fragmentation of mobile platforms and architectures leads to a diverse attack surface for an adversary. Enterprise app developers and IT departments, through EMM solutions, may enforce best practices for their apps, but by and large the attack surface remains. Samsung KNOX and Android for Work reduce this attack surface for many enterprises, but risks still remain and enterprises need to plan, provide remediation, and enable multiple layers of security.

Users within the enterprise now demand a mobile experience that is on par with or better than commercial apps. This presents app developers and IT organizations with a set of complex issues surrounding security, management, development, time-to-market, cost, performance, and user experience that need to be addressed.

Authentication

Mobile authentication is difficult; the username and password approach is insecure. This forces IT to impose long, complex passwords that hinder the user experience. Commercial apps leave security holes by leaving the user logged in. Users expect the same from their enterprise apps — a clunky authentication experience or a too heavily locked down app isn't likely to be well adopted by users. The solution is multi-factor authentication — something you know (e.g., password/PIN), something you have (e.g., tokens), and who you are (e.g., biometrics). Above multi-factor is context: policies to choose the right authentication measures based on environmental risks and past behaviors. However, both IT and developers are challenged with understanding the complexities and managing the time and cost of how various biometric and token-based authentication solutions will integrate with the back end and the app. Standards that abstract this complexity and enable the enterprise to move beyond passwords to more secure authentication measures have been developed and are being standardized.

App Development and Mobilization

The job of a mobile app developer has become increasingly complex. There are a spectrum of mobile devices and OSes; from smartphones, tablets, and wearables to Android, iOS, and Windows Mobile. In addition, developers need to prioritize the devices and OS to target; they also must struggle to decide which legacy applications they need to support for the mobile workforce. Time-to-market, cost, user experience, and app performance all factor into these decisions. Native, responsive web design (RWD), cross-platform, and app transformation/porting tools are available and have increasingly matured over the last few years. However, each tool has its benefits and drawbacks. IQT recently conducted a market survey on mobile app development, which included comparisons of the various mobile app development tools on the market today. We found that over the past few years, cross-platform tools have improved to provide better performance and better integration with the mobile platform. We believe that the enterprise should choose a cross-platform tool that provides native or native-like performance and the code should be portable. App transformation/porting tools simplify the porting of legacy desktop applications to run on a mobile device and are best used to provide a native-like app that follows business-specific workflows. Moreover, this market survey concludes that it is important for the developer and enterprise to understand the apps they need and choose the right tool for each project.

User Experience

Mobility is about experience. Apps that are overly complex, too restrictive, or perform poorly will quickly lose attention and relevance. Mobile app testing tools that are integrated with the development lifecycle for continuous integration allow developers to optimize the in-app experience before release. But these tools can only capture a subset of real world data points to test against. Other apps and services running alongside your app, as well as network, device, and OS variability are all events that are not easily testable. However, mobile application performance monitoring

(mAPM) tools that continuously report these events at runtime are accessible, and provide rich data about app performance, app crashes, and user experience. These tools enable developers to monitor, prioritize, troubleshoot, and trend mobile app performance to accelerate enterprise mobility and engage their users.

App Lifecycle Management

After building, acquiring, or mobilizing enterprise apps, managing the app's lifecycle is important for governance, development, and maintenance. Each stage of application lifecycle management (ALM) is necessary to ensure best practices are met to provide a robust, secure, and user accessible framework for enterprise app deployment. The ALM framework should allow the enterprise to easily on-board apps from app developers or through third-party app stores, inspect those apps to understand their behavior and report on potential risks, enable IT to enforce specific corporate security policies, and provide an enterprise distribution method that is capable of controlling app distribution and auditing app deployment and usage. This ALM framework should be extensible — allowing the enterprise to integrate with EMM and other tools within the enterprise IT infrastructure.

These are a few of the many challenges associated with enterprise mobile apps. IQT is engaging with companies offering solutions to these challenges, ranging from authentication methods and multi-factor authentication policy management platforms to mobile app development tools, enterprise app stores, and mobile app analytics. IQT will continue to engage with cutting-edge companies in this space to stay abreast of technology trends.

Mobility is increasingly prevalent and will continue it reach into the enterprise. As the IC continues to work through these challenges, it may be overwhelming, but it is an exciting opportunity. IQT will continue collaboration with our IC partners to define their mobile app strategies and focus on understanding and addressing challenges to refine a mobile architecture. Q

Isaac Myauo *is a Member of the Technical Staff within In-Q-Tel's Mobility Practice. Myauo's company portfolio includes investments in LTE small cells, mobile development and testing tools, and mobile communication technologies. Prior to IQT, he was with The MITRE Corporation. Previously, Myauo spent eight years at BAE in a variety of engineering roles, largely within mobility, tactical networking, and software-defined radio programs for DoD customers. Myauo received a bachelor's degree in Electrical Engineering from Drexel University and a master's degree in Systems Engineering from the Stevens Institute of Technology.*

A Look Inside: Planet of the Apps

This issue of the *IQT Quarterly* examines the recent advances and challenges associated with enterprise mobile applications. While the continued proliferation of mobile technologies has disrupted consumer and enterprise markets, it also presents IT organizations with a new set of issues ranging from security and authentication to development, user experience, and management.

Harvey Morrison of Apperian opens this issue with a discussion on the need to provide mission-critical mobile apps to government employees. Advances in mobile security and management techniques have broadened the possibilities for app deployment within many organizations, including those in highly secure settings.

Next, Phillip Dunkelberger of Nok Nok Labs explains the authentication issues created by Bring Your Own Device (BYOD) policies. Enterprises need to move beyond usernames and passwords to stronger, multi-factor authentication methods to allow employees to access real-time corporate data on mobile devices.

Todd Fryburger of StarMobile compares four approaches to mobile app development: buy, build, virtualize, and transform. Each approach faces challenges in time, complexity, and cost that have hindered enterprises in capitalizing on the potential of mobility.

Kevin Benedict of Cognizant continues with a discussion on the implications of mobile apps for the real-time enterprise. Today's users expect a fast, integrated mobile experience, and organizations must optimize their tempos to remain competitive.

Next, David Krebs of VDC Research shares perspectives on mobile application opportunities for public safety. In-vehicle and GIS apps are among the keys to improving mobility for first responders, but the influx of connected devices is creating IT challenges around security and management.

Andrew Levy of Crittercism closes the issue by examining the need to understand app performance. He argues that legacy testing approaches do not suffice for business- and mission-critical apps; instead, IT organizations should take a more holistic approach by monitoring adoption rate, responsiveness, crashes, and other metrics in real time.

Mobility continues to transform the enterprise IT environment, with a range of innovation taking place in established technology companies and smaller venture-backed startups. This issue of the *IQT Quarterly* aims to provide the Intelligence Community with an awareness of the challenges and opportunities presented by enterprise mobile applications. Q

How to Secure, Deploy, and Manage Mobile Apps in Highly Secure Settings

By Harvey Morrison

There is a clear need to provide mission-critical mobile apps to government employees. With smartphone adoption rates above 70 percent, these devices have become the computing platform of choice.[1] For many organizations, the focus of mobility is now to create apps that assist employees, contractors, and other knowledge workers to achieve mission objectives, improve productivity, and increase collaboration and communication.

The value of mobility for the Intelligence Community, in particular, can fundamentally change the playing field. Research analysts and intelligence systems benefit from timely information provided by field agents in near real-time. Similarly, field operators can benefit from curated intelligence information that is readily available on their mobile devices. It reduces the reporting lag and users don't have to wait until they are back in the office or on their laptops before mission-critical information is updated. Demand for such mobile apps is expected to accelerate, as shown in the IBM Institute for Business Value (IBV) study on Mobility Impact, which highlights that 63 percent of public sector respondents want mobile access to their specialized applications.[2]

When enabling teams — especially those in intelligence and other highly secure settings — ensuring data and mobile app security is essential. In the early stages of mobile development, a combination of built-in app security and device-level security measures, such as passcode complexity rules and on-the-fly disk encryption, were commonplace. For the early adopters of enterprise mobility, device security settings were handled by mobile device management (MDM) software. This approach continues to play a role, but it is only part of the puzzle.

This next phase in mobility is enabled with mobile application management (MAM), as emphasis shifts to the development and deployment of mission- and task-specific mobile apps. MAM provides comprehensive, fine-grained security, management controls, and usage visibility around individual apps – effectively bringing apps under management. The app security and management techniques built around in-house apps can also be extended to securing public apps, which allows an organization to take advantage of the larger app ecosystem while ensuring the appropriate level of security. This creates the most secure and manageable approach for delivering mobile apps and content at scale to knowledge workers in the field and regulated industries.

New Kinds of Mobile Apps, New Possibilities for Knowledge Workers

With trusted and secure mobile access to critical back-end systems established, work that previously required presence in a restricted office can now be accomplished in the field. Using an app- and data-centric approach to security and management allows agencies to create new applications and increases the range of knowledge workers that can take advantage of these innovations.

For example, communication and collaboration apps that capture information, such as location, photographs, content, voice, and more — much of that automatically captured and stored by the device and its knowledge of context — can provide a new lifeline of live streaming content. This can synchronize distributed teams and enable collaboration between agencies when responding to a crisis by enabling information sharing in the field.

App-centric security and management enable such scenarios because the apps don't just rely on a certain device security posture; they create a safe and compliant app space with an app-level security layer while still enforcing device security posture as appropriate. Why is this so critical? Because in some scenarios, there is now the ability to implement an additional app security layer that deals with data-at-rest, data-in-use, and data-in-flight encryption, in addition to device-level capabilities. In other scenarios, there is an increased desire to create and deploy apps to devices that are either not under device management with MDM software, such as for Bring Your Own Device (BYOD) devices or contracted workers, or devices that are being managed by MDM systems not under your direct control (such as intra-agency apps.)

Mobile App Lifecycle Management and Governance

As mobile apps continue to proliferate, organizations must deal with an environment where mobile apps are coming from many different sources. Selecting mobile apps, whether internally developed or sourced from third parties, allows an organization to keep pace with rapidly evolving mobile technologies and capabilities. Best-in-class mobile efforts will involve new apps being internally developed, developed by third-party app developers, or perhaps being provided by other agencies.

With varied sources and an increasing volume of mobile apps, organizations need a system of record — a way to apply standard vetting, security, and distribution processes and policies once apps are developed and before they are made available to their target audience to ensure organizational control, security, and adherence to best practices.

At a minimum, an organization's mobile app strategy and architecture should address:

- **Governance:** A platform to ensure that organizational standards are followed and applied
- **Security:** App-specific policies which operate at the app level to protect the app and its data, separately from device management and security
- **Integration:** Into key enterprise systems such as identity, build, and event tracking
- **Deployment:** A flexible model to support the broadest number of users and mobile OS choices

As organizations continue to develop a greater number of mobile apps, both internally developed with their own resources and via contracted third parties, having a stand-alone, standard governance and security platform to vet, secure, and deploy these apps is crucial for organizational control and security. The app and governance platform should provide a central, controlled system to manage the app and its lifecycle.

This enables organizations to safely and swiftly on-board and iterate mobile apps to respond to user needs. An app lifecycle approach establishes guidelines for app development and a platform for on-boarding apps from any source, consistent app inspection, a standardized method for deploying apps to users, and analytics into app adoption, usage, and performance.

Mobile app lifecycle management.

Advances in mobile security and management techniques have made new kinds of apps and broad deployment within reach for most organizations — even those with the highest levels of security.

App On-Boarding: Organizations should have a standardized approach for on-boarding mobile apps, regardless of their source. This should include integration with popular mobile app development platforms (MADPs) as well as app build platforms, such as Jenkins, and the ability to simply upload compiled mobile apps, which may be internally developed or provided by third parties. App on-boarding should be simple for IT administrators — this leads to timely access to the latest innovations for users.

App Inspection: With mobile apps being sourced from a wider variety of suppliers, inspecting the app's code for malware and other malicious or risky behavior is essential. This should catch dangerous code, such as viruses, and flag behaviors such as location services or poor programming choices that unnecessarily tax the device hardware. With a consistent inspection approach, the organization can accept or reject apps based on established standards.

App Protection and Policy Management: After app inspection and following the organization's governance processes, security and management policies should be applied. The best practice approach is to apply such policies via app wrapping, which takes an app executable and adds standardized application policies, resulting in an app with new security, administrative, and management capabilities. These policies can encapsulate any mobile app without requiring modifications to the app's code. As a result, mission-critical apps can be deployed and operated securely in the field — even on commercially available off-the-shelf hardware.

There are significant governance benefits that this approach affords. First, it abstracts the complexity for an app developer when implementing security methods and allows the developer to focus on adding business value, while the security community can focus on a common app security and compliance posture. Second, and closely related, organizations can easily apply consistent security policies across a range of apps without requiring the same, duplicative coding effort for each. This is the scalable approach to ensure consistent security and management for all apps across the entire organization.

Examples of app-level security policies include enterprise authentication, two-factor authentication, app-level VPN, data-at-rest and data-in-use encryption, app expiration, copy/paste disable, self-updating apps, jailbreak detection, app usage and analytics, and more. This provides an opportunity for an organization to use its own preferred encryption methodology or Federal Information Processing Standard (FIPS) compliance libraries. Many agencies may want to integrate their apps with identity management systems as well as Common Access Card (CAC) and Personal Identity Verification (PIV) technology to enable two-factor authentication. These fine-grained controls enable administrators to ensure that apps are used only by authorized individuals and in the manner intended.

In addition to the security and management benefits of wrapping and deploying apps with policies, organizations seeking the highest-level of data security may also consider integrating those apps with secure elements on the mobile device. Such secure elements can provide support for two-factor authentication and may be in the form of removable micro SD cards, components that can be plugged into a USB port, or components built directly into the device. Secure elements can contain crypto chips, which provide basic crypto primitives for generating encryption keys, encrypting and decrypting small data sets, and generating reliable random number sequences. With this combined technique, the apps are now secured

through two-factor authentication. Without both the secure element and the PIN, the apps will not run.

App Signing: An often-overlooked complexity for app developers and administrators is the requirement to sign all apps before they can be deployed to a user's device. In Apple's iOS environment, signing an app is when the app developer applies his or her enterprise credentials provided by Apple to the app. This is a way of signaling to the mobile device that it is a legitimate, trusted app and, therefore, allowed to run. Signing must occur after each app is updated, compiled (or recompiled), and distributed — before users can install and run it. Additionally, every iOS app must also be re-signed every 12 months to reconfirm that it is deployable.

Organizations should have a centralized way to manage app signing credentials and processes. An app signing facility can allow any authorized administrator to sign an app from an admin console and prepare it for deployment without requiring time or effort from a developer. This greatly reduces the time and complexity of signing apps while enabling the signing process to be repeated easily with predictable results.

App Deployment: With one or more mobile apps on-boarded, inspected, signed, and secured, administrators need an easy way to deploy them into production for end users. For most organizations, a custom-branded, private app store is the optimal mechanism to display and distribute apps under management. Users can be tiered according to any number of factors, including role, work team, and security clearance. Following the best practice approach of app-centric security and management, private app stores should be securely reachable by users regardless of who controls and manages the device. This will be required for apps deployed to broader teams, other agencies, contracted workers, and others using unmanaged devices. Because the private app store is independent of device management, there are no issues having a single, centralized app distribution strategy.

Mobile App Security and Deployment Now Ready to Support the Mission

There is unquestionable value in enabling government knowledge workers with mobile apps and access to critical systems. Mobile devices are the platform of choice for users. Their processing power is increasing and reliable network coverage is improving. Security requirements have historically been a limiting factor that has slowed innovation for front-line workers. However, advances in mobile security and management techniques have made new kinds of apps and broad deployment within reach for most organizations — even those with the highest levels of security. The result can be government teams moving with agility not recently possible, and creating and deploying innovative apps to make secure data collection, consumption, and collaboration a reality. Q

Harvey Morrison *heads the Public Sector business for Apperian, a leading mobile application management and app security company. He is responsible for leading and managing all customer-facing activities and he frequently speaks on mobile management and security best practices. Earlier in his career, Morrison led the public sector team for Endeca through its acquisition by Oracle, and for Verdasys. He also held public sector sales leadership positions at Enigma and Parametric Technology Corporation (PTC). He holds a Bachelor of Science in Business Administration from The Citadel.*

REFERENCES

[1] http://www.asymco.com/2014/07/08/late-late-majority/
[2] https://ibmexperts.computerwoche.de/sites/default/files/studie-ibv-institute-business-value_0.pdf

The Changing Nature of Authentication: Meeting the Needs of Mobile Enterprise Applications

By Phillip Dunkelberger

The way the modern enterprise consumes applications and data is changing. We have moved from a PC-centric model, where users access corporate data through a browser, to native mobile applications on smart devices. This change has been accompanied by a fragmented device ecosystem, with employees playing increasingly significant roles in selecting the devices they use to access corporate networks.

The inevitable switch to Bring Your Own Device (BYOD) has its benefits and consequences. In an environment where enterprise data is delivered to smart devices by native mobile applications, our security models need to change. Employees will need to be able to access corporate applications and information in the same way they would access their mobile banking or cloud storage apps. In order to achieve the ability for employees to remotely access corporate applications and information, authentication frameworks and approaches will need to be reexamined and updated.

Like many other foundational areas of information technology, the authentication sector finds itself at a crossroads: it needs to move beyond usernames and passwords to stronger, more accurate identifiers that are applicable in modern computing. While this has been recognized as a necessity, we still find ourselves struggling with how to best secure access to information across the broad range of devices we use today. How we authenticate to a device or service is how we first engage with it, so it shapes our user experience, both positively and negatively. Authentication is not only about security, it is also about engagement, ease-of-use, and user experience. Unfortunately, current authentication frameworks result in more secure devices being harder to use.

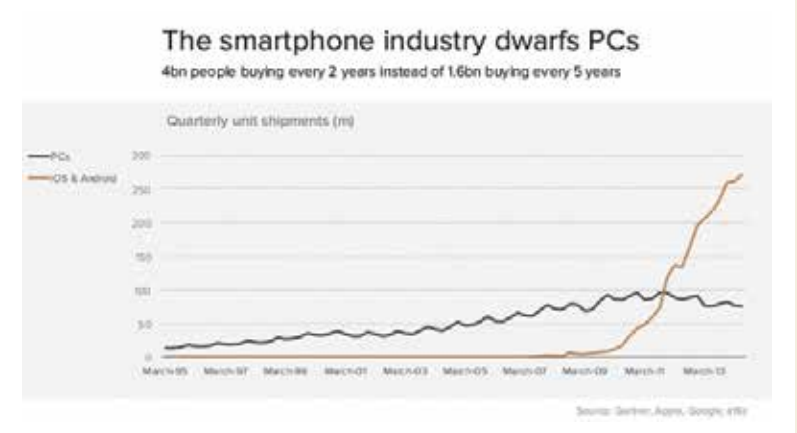
The need for online authentication started 50 years ago, with the introduction of passwords to secure access to mainframe computers.[1] Since the early 1960s, the industry has seen an extraordinarily diverse range of technologies deployed to augment or attempt to replace the humble password — hardware tokens, grid cards, fingerprints, heartbeat, and even a pill that the user swallows.[2] Even with these varied technologies, we still remain highly dependent on usernames and passwords to navigate the corporate world, the Internet, and native mobile applications.

Defining potential solutions to modern authentication needs requires a shared understanding of

authentication fundamentals. Generally, both consumer and enterprise authentication have been based on weak or basic authentication. This is effectively synonymous with the use of a password. As employees and customers, we have been trained to establish usernames — typically an email address or employee ID, followed by a secret password — and that is where the process becomes complicated. Depending on the application, or policy, that password might be between 8 and 20 characters long, have specific requirements around unique characters, and need to be reset every 60 to 120 days.

The challenge with this model is that we are not equipped to remember multiple, complex passwords, so we tend to take the path of least resistance. We repeat the same passwords across multiple applications, which creates a massive security risk within organizations. If I use the same credential for a social network application that I use to access confidential company databases, then a data breach at that social network can have a direct impact to my company's security profile. It doesn't matter if the firewalls are running properly, or that antivirus protection is up-to-date. If an attacker has valid credentials, all of the main external-facing defenses will be bypassed. Researchers at the University of Cambridge analyzed the password databases from a number of large public data breaches and found that up to 76 percent of them were reused across multiple applications.[3] This, more than anything else, is why the password can no longer be seen as an appropriate credential for accessing enterprise resources.

Passwords also have a significant impact on employee productivity and operational cost. What was acceptable in the traditional desktop computing model has become untenable when we are consuming services through native mobile applications. The transition to mobile first as a way of delivering enterprise applications means that the authentication landscape has to change to reflect the nature of the devices on which we consume and create data. Typing in long, complex, constantly changing passwords on small, touchscreen devices is a struggle for employees and the constant need to reset passwords results in significant help desk costs. A vendor survey suggests that 20 to 50 percent of all help desk calls are related to password resets and that the average labor cost for one password reset is $70.[4]



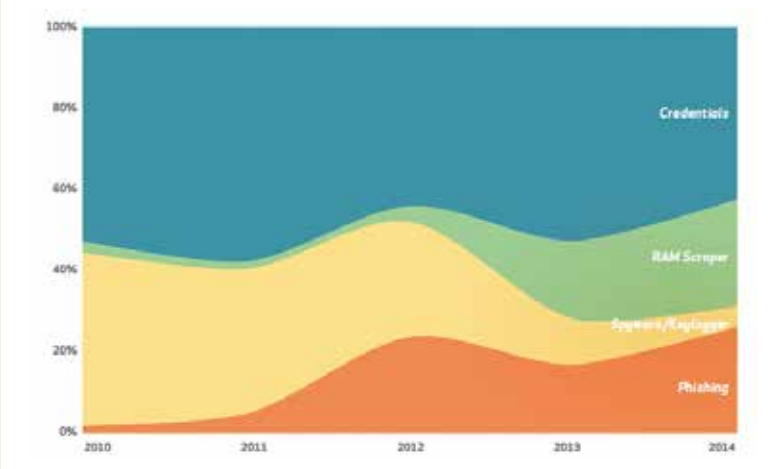
Quarterly unit shipments, 1995 - 2013: PCs vs. iOS & Android.

Since the password has no long-term future as a method of accessing data on mobile applications, what is the alternative? We are left with strong or multi-factor authentication. The standard industry definition of multi-factor is that it consists of:

- **Something you have:** such as a separate hardware token, typically used for enterprise authentication or in consumer banking; this could equally be a mobile device or a smartcard.
- **Something you know:** this could represent a password or passcode, or it could be information only the user is supposed to know — e.g., your mother's maiden name or Social Security number.
- **Something you are:** a unique biometric identifier, such as a fingerprint.

In order for the authentication to be strong, it should consist of two of these factors and all of the factors must be independent. Thus, the compromise of one factor does not result in the breach of another.

The recent publication of the Verizon Data Breach Investigations Report (DBIR) for 2015 highlighted some interesting findings with regards to mobility and authentication. It suggested that, while the mobile channel represents a serious theoretical risk, the real threat associated with data breaches still comes from vulnerable web applications and point-of-sale (POS) systems, with malware-infected smartphones on the Verizon network equaling less than 0.03 percent per week.[5] It also showed the extent to which compromised credentials have become a problem. We are all aware of high profile incidents where authentication failures



have resulted in significant data breaches. This was apparent at Target, where an external supplier's password was used as a first point of entry in order to escalate privileges internally, which resulted in significant fiscal and reputational damage and cost the Target CEO his job. In fact, the DBIR shows that nearly half of all malware attacks were focused on stealing authentication credentials for reuse.

Considering that this is the threat landscape, why has the adoption of strong authentication been so piecemeal? There are many answers to that question, but we can break it down into the two main areas we've touched on previously: cost and usability.

Analyzing the cost of deploying strong authentication requires a consideration of all of the factors involved, not only the cost of acquiring the software or hardware associated with the rollout. As discussed previously, costs of account recovery must be factored in, as well as the costs of distribution in the case of hardware tokens. Figures show that the ongoing costs of deploying strong authentication can significantly multiply the total cost of ownership. This explains why organizations have historically adopted a narrow and fragmented approach to strong authentication, limiting it to critical scenarios, such as access to financially sensitive information or commercially important data such as source code. However, the spread of data within companies has made us all custodians of sensitive information, and traditional Data Loss Prevention (DLP) tools have struggled to keep up as we move more and more of our corporate data to cloud services, accessed remotely via a range of tablets and smartphones.

The other significant barrier is usability. The adoption and use of traditional strong authentication solutions have required a degree of effort from the employee. As we transition to the mobile and application-centric model, the expectation is that this complexity and friction should be significantly reduced or eliminated if we want to scale strong authentication across all applications within the enterprise. We have established that the smartphone/app model does not lend itself well to password-based authentication, nor does it play well in a hardware token-based architecture. What might seem reasonable in the traditional, browser-based computing framework will not necessarily be applicable in a mobile-centric world given the constraints imposed by smartphones and tablets.

For a while, enterprises were able to look at the mobile device itself as the authentication tool — employees could either generate a one-time passcode (OTP) on a specific application, or have it delivered to them via SMS. This would then allow them to login to the appropriate session on another device. The reality today, however, is that the mobile device is the primary transaction vehicle, so it cannot act as an independent channel for strong authentication.

Device-Centric Models

The evolution of the modern smartphone presents us with some new possibilities in the future of authentication. Today's mobile devices offer many of the security assurances previously offered only in smartcards. These credentials can be bound to a specific user via a number of methods, such as passcodes and biometrics. Other smartphones may offer similar assurances, such as Apple's Secure Enclave or Trusted Platform Modules (TPM) on Windows Mobile devices. These secure areas are malware-resistant and provide IT security organizations with the level of granularity they need to support remote access to internal network services. A good example of this can be seen with Samsung KNOX.

In addition to these smartcard-like capabilities, device manufacturers are increasingly investing in innovative user verification capabilities. Apple was the first western device manufacturer to introduce a fingerprint sensor (FPS) across a broad range of devices with the

Apple 5S in September 2013. Samsung followed with the Galaxy S5 in April 2014.

These devices all allowed the user to create a biometric template, maintained locally on the device in a secure environment, that could be leveraged by enterprise applications to authenticate the user and the device. As users become accustomed to these capabilities, it seems natural to allow them to access enterprise apps, provided that the business is able to apply the appropriate safeguards. We are now moving from BYOD to BYOA — Bring Your Own Authenticator.

There are advantages that the BYOA approach can provide the enterprise. First, enterprises are not trying to force their users into unusual patterns of behavior and, secondly, they are not required to acquire and distribute the authenticator, as the smartphone manufacturer has already built it in.

However, in order for an enterprise to truly take advantage of the different capabilities delivered to market across a wide range of devices, they need to have a clear understanding of the security characteristics of these devices. How do they capture the fingerprint, iris scan, or voice recording? How do they store this information on the device? How can the app easily integrate with different methods of authentication (biometric or non-biometric) across different devices?

This is where the work of the FIDO (Fast IDentity Online) Alliance should be of particular interest and may have a unique impact. The FIDO Alliance is an industry non-profit working group with a mission to define a strong authentication standard that enables a broad range of device-centric user verification methods, supported by a strong, cryptographic protocol between the device and the enterprise web application. By standardizing these elements, the FIDO protocols can enable the broad adoption of a wide range of natural authentication methods across any number of different devices — while providing the ability and functionality to be controlled and managed by the enterprise.

If we aim to allow employees to access real-time corporate information via mobile applications in order to increase productivity and reduce operational cost, then we need to solve the fundamental authentication problems. The work and mission of the FIDO Alliance is focused on addressing these issues, and represents the next wave of modern computing, where we accept the devices that an employee brings to the enterprise, with the ability to leverage the authentication methods and capabilities they already have to support secure access to corporate data, instead of imposing a rigid, inflexible structure that cannot scale to meet the needs of the modern and distributed enterprise. Q

***Phillip Dunkelberger**, President and CEO of Nok Nok Labs, has broad technology experience resulting from more than 30 years in the industry. Prior to leading Nok Nok Labs, Dunkelberger served for eight years as co-founder and CEO of PGP Corporation, the leader in the enterprise data protection market, until its acquisition by Symantec in 2010. He has significant experience in SaaS infrastructure and enterprise software, having served as Entrepreneur-in-Residence at Doll Capital Management (now DCM), President and CEO of Embark, and COO of Vantive Corporation. He has also held senior management positions with Symantec, Apple Computer, and Xerox Corporation. He is a founding board member of the Cyber Security Industry Alliance (CSIA) and is Chairman Emeritus of TechAmerica's CxO Council. Dunkelberger holds a B.A. in Political Science from Westmont College and is a member of the school's President's Advisory Board.*

REFERENCES

[1] http://blogs.wsj.com/digits/2014/05/21/the-man-behind-the-first-computer-password-its-become-a-nightmare/
[2] http://www.entrepreneur.com/article/231182
[3] https://www.lightbluetouchpaper.org/2011/02/09/measuring-password-re-use-empirically/
[4] https://www.noknok.com/sites/default/files/whitepapers/4barrierswhitepaper_0.pdf
[5] Verizon, DBIR, 2015

Enterprise Mobile Apps: A Promise Unfulfilled

By Todd Fryburger

The consumer mobility market has experienced massive growth, largely driven by the sale of smartphones, which topped 1.2 billion units sold globally in 2014, a 28 percent increase from 2013.

This consumer adoption subsequently drove the Bring Your Own Device (BYOD) movement, as employees demanded the right to bring personally owned mobile devices into their workplaces. Ninety-five percent of employees now report that they use at least one personal device for work. In turn, companies adopted mobile device management (MDM) solutions for security and control, largely to protect company information and applications. This resulted in companies locking down employee devices to provide secure access to Personal Information Management (PIM) applications such as email, calendar, and contacts.

However, despite the ascent of mobile devices in the workplace, fewer than 25 percent of companies have built or bought a mobile app beyond PIM apps. Despite the high demand from employees to access corporate systems from mobile endpoints, enterprises are woefully unable to deliver the consumer-like user experiences their employees expect.

Where Are All the Apps?

The average Global 2000 enterprise uses 424 packaged and custom-built applications to support its business.[1] This includes packaged on-premises applications such as SAP, Oracle, IBM, and Microsoft, packaged cloud-based applications such as Salesforce and Workday, and bespoke applications that were purpose-built using Web, .NET, Java, and even legacy "green screen" systems.

Regrettably, less than 5 percent of these applications have been extended to users on mobile devices due to the excessive time, complexity, and cost to mobilize them. For example, on average, companies report that it takes seven months and $270,000 to develop one mobile app of medium complexity for two mobile device platforms (e.g., iOS and Android).

According to Gartner, companies need to be prepared to develop and support up to 2,000 mobile apps over the next three to five years, as the mobilization of a given back-end system will likely yield multiple apps to support various subsets of workflows.[2] This means the enterprise is facing a potential of 1,000 or more person-years of work at a cost greater than half a billion dollars to simply extend such systems to users on mobile devices.

Sadly, only 33 percent of companies report that they have a formal strategy for enterprise mobility. Further, 67 percent of CIOs report they have no specific budget for such projects, 53 percent have infrastructure built

for Web (not mobile), and 50 percent do not have the right tools and skills in-house to develop mobile apps. Clearly, the time, complexity, and cost of current approaches have relegated enterprise mobility as "a promise as yet unfulfilled."

Blame the Vendor Community, Not the CIO

To be fair, the CIO should not shoulder the blame alone for this lack of progress. Rather, the technology vendor community shares responsibility, as the solutions and approaches that have been set forth to date are slow, complex, and expensive, relegating enterprise mobility as a luxury that can only be justified by a handful of revenue-generating or customer-facing use cases.

Such approaches can be broken down into four categories: Buy, Build, Virtualize, or Transform.

Buy

Some companies hold hope that they can Buy mobile apps from current on-premises or cloud-based application vendors, or will receive them as part of future upgrades under their maintenance contracts. Regrettably, less than 23 percent of companies implement such systems off-the-shelf without customization. Therein, if a customer wishes to use the mobile apps provided by that vendor, they need to modify the source code of that app to reflect the customization to the associated back-end application. The result is that Buy is likely the slowest, most complex, and most expensive choice a customer could make, because it involves customization on the back end and the mobile app.

Build

The majority of vendor solutions are in the Build category. It is important to note that on a percentage basis, mobile apps are perhaps the most time consuming, complex, and expensive to create, support, and maintain in all of IT. Compared to other technologies, where ongoing support and maintenance roughly equates to 20 percent annually of the original amount invested in the application, mobile apps require more than 50 percent, largely due to the accelerated technology churn and diversity of mobile device platforms.

Build options include native mobile operating systems such as iOS, Android, Windows Mobile, and BlackBerry, as well as open source mobile platforms. Native and open source are fine if a company is building an app for a specific mobile device, but time, complexity, and cost issues increase exponentially when a company needs to build and maintain multiple apps across multiple mobile operating systems and form factors.

Build solutions also include Mobile Application Development Platforms (MADPs). MADPs were created based on the notion that mobile apps for the enterprise could be developed and managed using a singular platform. However, MADPs are proprietary development tools that require exotic skill sets and fluency in those tools, which in turn typically creates a dependency on external consultants to implement and maintain apps created using those platforms, unless the enterprise invests in hiring, training, and retaining those resources themselves. In addition, MADPs often present high software licensing and maintenance costs, which is why MADPs have already become a legacy approach before they have gained critical mass in the market.

It is important to note that the "holy grail" of mobile app development is "write once, run everywhere," or rather, cross-platform support for developing native apps. However, Build tools that promise platform ubiquity present significant trade-offs, particularly with respect to suboptimal user interface and poor performance. In general, such tools are better described as "write once, debug everywhere."

Another Build category that has recently emerged is Mobile Back end as a Service (MBaaS). Such MBaaS solutions provide mobile developers with a way to link apps to application programming interfaces (APIs) to back-end applications. It remains, however, the MBaaS tools are middleware between app and back end, which means the customer must either build a native app or platform-based app on the mobile device. Further, this assumes that companies have developed structured API libraries, of which few have invested the time, resources, and money to complete. It remains of question as to whether MBaaS is really a Build tool category, as it is limited to API aggregation.

A final Build category has emerged recently, called Rapid Mobile Application Development (RMAD). RMADs are designed to address the time, complexity, and cost challenges of mobile app development, and present alternative, faster approaches that yield rapid delivery by a wider range of lower-cost resources. This market is being driven by significant innovation, with the objective to replace traditional coding with more effective codeless development tools that automatically build the constructs of the mobile app. Some of these tools permit resources without coding skills to create mobile apps, such as analysts at the line of business.

Complexity	Step	Number of Mobile OS		
		One	Two	Three
Low	Design	40	70	105
	Develop	120	240	360
	Test	40	78	116
	Validate	20	39	58
	PM	55	107	160
	TOTAL	**275**	**533**	**799**
Medium	Design	80	140	210
	Develop	240	480	720
	Test	80	155	233
	Validate	40	78	116
	PM	110	213	320
	TOTAL	**550**	**1,066**	**1,598**
High	Design	160	280	420
	Develop	480	960	1,440
	Test	160	310	465
	Validate	80	155	233
	PM	220	426	639
	TOTAL	**1,100**	**2,131**	**3,197**

Figure 1 | Traditional app development (man-hours).[3]

Complexity	Step	Number of Mobile OS		
		One	Two	Three
Low	Design	23	29	35
	Develop	13	16	19
	Test	6	8	9
	Validate	3	4	4
	PM	5	7	8
	TOTAL	**50**	**63**	**76**
Medium	Design	47	58	70
	Develop	25	32	38
	Test	12	15	18
	Validate	6	7	9
	PM	11	13	16
	TOTAL	**101**	**126**	**151**
High	Design	93	116	140
	Develop	51	63	76
	Test	24	30	36
	Validate	12	15	18
	PM	22	27	32
	TOTAL	**202**	**252**	**302**

Figure 2 | New approaches to app development (man-hours).[3]

RMADs hold considerable promise for the future of the Build approach to enterprise mobility. However, there is a huge variation in the various RMAD vendor offerings. Many are newer solutions that are continuing to evolve, yet are incomplete, and in an increasingly crowded field where no clear leaders have emerged.

Virtualize

Virtualization solutions have been offered by established players for many years. These are based upon remote computing protocols that are 20 to 30 years old, which provide the means to revisualize applications between homogeneous desktop environments. Whereas the major benefits of virtualization are speed, security, and low cost, the drawback is a poor, non-native user experience, which is particularly acute when using a mobile device.

Transform

Virtualization has given rise to new tools that apply next-generation technologies to refactor or transform the back-end application for consumption on mobile devices. Therein, such solutions deliver the speed, security, and economy of virtualization, but also deliver a native user experience on the mobile device.

Most app refactoring solutions specialize in virtualizing a specific class of back-end technologies, such as Web, .NET, Java, or green screens, and then can only address a portion of the application functionality built on those technologies. However, only a handful of solutions have recently emerged that transcend any application based on any back-end technology to any endpoint.

Comparing Approaches

When selecting an enterprise mobility solution that is best for your organization, it is important to evaluate the time, complexity, and cost considerations.

Complexity in mobile app development comes in many forms. On the client side, this includes the number of apps, rate of change for apps, diversity of mobile OS, devices, and form factors, online/offline synchronization, geography, and even carrier. For back-end integration, this includes diversity of applications, e.g., on-premises, cloud, or bespoke (Web, .NET, Java, etc.), infrastructure such as APIs, data connectors, SQL, web services, MBaaS, content management, and security. One must consider the resources and skills required across each of these elements.

Complexity	Step	Number of Mobile OS		
		One	Two	Three
Low	Design	$10,000	$17,500	$26,250
	Develop	$30,000	$60,000	$90,000
	Test	$10,000	$19,375	$29,063
	Validate	$5,000	$9,688	$14,531
	PM	$13,750	$26,641	$39,961
	TOTAL	**$68,750**	**$133,203**	**$199,805**
Medium	Design	$20,000	$35,000	$52,500
	Develop	$60,000	$120,000	$180,000
	Test	$20,000	$38,750	$58,125
	Validate	$10,000	$19,375	$29,063
	PM	$27,500	$53,281	$79,922
	TOTAL	**$137,500**	**$266,406**	**$399,609**
High	Design	$40,000	$70,000	$105,000
	Develop	$120,000	$240,000	$360,000
	Test	$40,000	$77,500	$116,250
	Validate	$20,000	$38,750	$58,125
	PM	$55,000	$106,563	$159,844
	TOTAL	**$275,000**	**$532,813**	**$799,219**

Figure 3 | Traditional app development (costs).[3]

Complexity	Step	Number of Mobile OS		
		One	Two	Three
Low	Design	$4,362	$5,453	$6,544
	Develop	$2,369	$2,962	$3,554
	Test	$1,137	$1,421	$1,705
	Validate	$560	$700	$840
	PM	$1,009	$1,261	$1,513
	TOTAL	**$9,437**	**$11,797**	**$14,156**
Medium	Design	$8,725	$10,906	$13,087
	Develop	$4,739	$5,923	$7,108
	Test	$2,273	$2,842	$3,410
	Validate	$1,121	$1,401	$1,681
	PM	$2,017	$2,521	$3,026
	TOTAL	**$18,875**	**$23,593**	**$28,312**
High	Design	$17,450	$21,812	$26,175
	Develop	$9,477	$11,847	$14,216
	Test	$4,547	$5,683	$6,820
	Validate	$2,241	$2,802	$3,362
	PM	$4,034	$5,043	$6,051
	TOTAL	**$37,749**	**$47,187**	**$56,624**

Figure 4 | New approaches to app development (costs).[3]

	Solution Element	Year 1	Year 2	Year 3	Totals
Development	Initial App Work Effort	$599,414	$0	$0	$599,414
	Ongoing App Work Effort	$299,707	$299,707	$299,707	$899,121
	Training	$29,971	$5,994	$5,994	$41,959
	App Support	$149,854	$149,854	$149,854	$449,561
Software	Mobile SaaS Subscription	$0	$0	$0	$0
	Mobile Platform Software	$250,000	$0	$0	$250,000
	Mobile Development Tools	$25,000	$0	$0	$25,000
	Mobile Testing Tools	$25,000	$0	$0	$25,000
	Mobile Software Maintenance	$60,000	$60,000	$60,000	$180,000
Infrastructure	Infrastructure Hardware	$21,900	$0	$0	$21,900
	Infrastructure Hardware Maintenance	$4,380	$4,380	$4,380	$13,140
	Infrastructure Software	$4,380	$0	$0	$4,380
	Infrastructure Software Maintenance	$876	$876	$876	$2,628
	Space and Racks	$7,300	$0	$0	$7,300
	Ping, Power and Pipe	$5,475	$5,475	$5,475	$16,425
	Vendor Management	$4,431	$4,431	$4,431	$13,293
	Infrastructure Support	$11,078	$11,078	$11,078	$33,233
	TOTALS	**$1,498,765**	**$541,795**	**$541,795**	**$2,582,354**

Figure 5 | Traditional app development: total cost of ownership (TCO).[3]

	Solution Element	Year 1	Year 2	Year 3	Totals
Development	Initial App Work Effort	$0	$0	$0	$0
	Ongoing App Work Effort	$0	$0	$0	$0
	Training	$0	$0	$0	$0
	App Support	$29,971	$29,971	$29,971	$89,912
Software	Mobile SaaS Subscription	$233,643	$233,643	$233,643	$700,929
	Mobile Platform Software	$0	$0	$0	$0
	Mobile Development Tools	$0	$0	$0	$0
	Mobile Testing Tools	$0	$0	$0	$0
	Mobile Software Maintenance	$0	$0	$0	$0
Infrastructure	Infrastructure Hardware	$1,095	$0	$0	$1,095
	Infrastructure Hardware Maintenance	$219	$219	$219	$657
	Infrastructure Software	$219	$0	$0	$219
	Infrastructure Software Maintenance	$44	$44	$44	$131
	Space and Racks	$365	$0	$0	$365
	Ping, Power and Pipe	$274	$274	$274	$821
	Vendor Management	$222	$222	$222	$665
	Infrastructure Support	$554	$554	$554	$1,662
	TOTALS	**$266,605**	**$264,926**	**$264,926**	**$796,456**

Figure 6 | New approaches to app development (TCO).[3]

As with most IT projects, mobile app development can be broken down into Design, Develop, Test, Validate, and Project Management steps. The person-hours associated with each of these steps will vary based upon the complexity of the app, ranging from low to high. In addition, these hours will also vary based upon the number of mobile operating systems the app must support.

Figure 1 shows the typical man-hours associated with traditional app development, including native, open source, and MADP-based app development. In this example, it requires 1,066 hours to complete a mobile app of medium complexity for two mobile operating systems (e.g., iOS and Android). In contrast, Figure 2 represents the typical hours associated with using new approaches, such as RMADs.

Therein, the same medium complexity app for two mobile operating systems can be rendered in 126 hours, which is less than 12 percent of the hours associated with a traditional approach.

Based upon prevailing internal IT resource costs, Figure 3 illustrates the costs associated with traditional app development. In this example, it costs $266,406 to complete a mobile app of medium complexity for two mobile operating systems. Accordingly, Figure 4 sets for the costs associated with new approaches.

Total Cost of Ownership (TCO)

As previously stated, on a percentage basis, mobile app development is perhaps the most time consuming and expensive type of development. In contrast to most IT projects, where ongoing support and maintenance is about 20 percent of the original development cost per year starting in the first year, traditional mobile app development is 50 percent, largely due to the rapid rate of change in mobile devices and mobile operating systems.

A comprehensive TCO model incorporates all elements required to design, develop, test, validate, support, and maintain a mobile app, as well as the related software and infrastructure costs over a three-year period. Figure 5 illustrates such a TCO analysis that a leading consumer products company developed for purposes of evaluating various approaches to traditional app development.

Despite the high demand from employees to access corporate systems from mobile endpoints, enterprises are woefully unable to deliver the consumer-like user experiences their employees expect.

In this example, the three-year TCO using traditional approaches is $2,582,354. By way of comparison, Figure 6 illustrates the TCO for analysis using new approaches to mobile app development.

Therein, the TCO for the same app using new approaches is $796,456, which is about 30 percent of the TCO as compared to a traditional approach. Of course, there is no one size fits all approach for developing such a TCO analysis, but these examples should provide a framework that any company can build upon.

Summary

Whereas the growth of enterprise mobility has been inhibited by time, complexity, and cost issues, vendors are rising to the challenge by creating next-generation tools to help companies address the need to render apps quickly, simply, and economically.

As consumers of mobile technology, we live in a world of 99 cent apps, which is simply not applicable to the mobile demands of the enterprise. However, this next generation of solutions is quickly helping to bridge the gap, a massive step towards fulfilling the promise of enterprise mobility. Q

Todd Fryburger, *President and CEO of StarMobile, has more than 30 years of experience in enterprise software and enterprise mobility for respected technology industry leaders, including Cramer Systems (acquired by Amdocs), PeopleSoft (acquired by Oracle), CSC, Chrysler Systems (acquired by IBM), GE Information Services (acquired by OpenText), and CompuServe (acquired by AOL). Fryburger previously served as the CEO of enterprise mobility leader CAS AG (acquired by Accenture). He most recently led Global Enterprise Mobility for SAP.*

REFERENCES

[1] http://www.zdnet.com/article/enterprise-mobility-in-2014-app-ocalypse-now/, http://www.vansonbourne.com
[2] Gartner Presentation, "Magic Quadrant: Mobile Application Development Platforms", Van Baker, IT Symposium October 2014.
[3] http://www.kinvey.com/2014-mobility-survey-report

Mobility, Operational Tempos, Information Strategies, and the Real-Time Enterprise

By Kevin Benedict

In a recent survey of 80 IT and business professionals, 73 percent responded that having optimized mobile applications and user experiences was "very important to critical" to their company's future success.[1] In the same survey, however, 78 percent reported their mobile strategies and plans were inhibited or limited by their existing IT environment. These results reveal a critical gap between the requirements for success and the reality of the obstacles enterprises are facing. Overcoming these challenges is the strategic imperative facing large enterprises today.

Enterprises understand that digital transformations being driven by mobile technologies and the Internet of Things (IoT) are changing their industries and markets. Consumer behaviors are changing at speeds never before seen, which impacts how businesses operate and bring products to market. These rapid changes are forcing enterprises to change their strategies in R&D, manufacturing, distribution, marketing, and sales. They are being forced to reconsider budget priorities and plans. They feel uneasiness. They are concerned with their ability to remain competitive, to understand real-time market trends, and to be agile and flexible enough to respond in time. They do know, however, that mobile technologies, sensors, and information management are at the forefront of these changes and are key components of any plans and strategies.

Real-Time Enterprises and Mobility

As organizations begin developing mobile strategies and implementing mobile apps, they quickly realize that simply developing and deploying basic mobile apps, infrastructure, and frameworks are not enough. They must push further and implement a real-time enterprise to remain competitive. This real-time requirement is at the root of many additional challenges. Eighty-four percent of survey participants reported that they have IT systems too slow or incapable of supporting real-time mobility, which negatively impacts mobile app performance and user experience.[1]

Jonathan Gabbai, Head of International Mobile Product at eBay, recently reported that almost half of eBay's transactions globally are now touched by mobile.

Users conduct product research, create wish lists, and complete transactions using mobile applications. With so much business now depending on mobile device, application, and website performance, the user experience must be outstanding in order to be competitive. An October 2014 Harris Poll survey found that 37 percent of U.S. smartphone and tablet owners now favor mobile shopping over in-store shopping, and Google reports that 79 percent of consumers now say they use a smartphone to help with shopping.[2] These numbers alone should move mobile technologies up the priority list of any business.

Although an increasing number of shoppers prefer the convenience of mobile shopping, they still remain hard to please. Forty-six percent of mobile shoppers say they will leave a mobile app or mobile site if it fails to load in three seconds or less, while 80 percent will leave if the mobile app or site is buggy or slow.[2] Consumers' expectations on what defines a good user experience are changing fast, but seem always to begin with speed.

Operational Tempos and Mobility

Supporting real-time mobility is more than just a technology issue. It also requires companies to support real-time operational tempos. An operational tempo, in the context of this article, is defined as the speed or pace of business operations. Achieving a satisfactory operational tempo in order to support real-time mobility is a significant challenge and extends far beyond the IT environment and deep into decision-making and business processes.

Changing an enterprise's operational tempo requires strong leadership that can transform the entire organization. It often requires significant IT updates and upgrades, organizational changes, and reengineering business processes and decision-making matrixes to align with real-time demands.

The military strategist and U.S. Air Force Colonel John Boyd taught that in order to win or gain superiority over an opponent, one should operate at a faster tempo than the opponent. Today competition is increasingly around the quality of mobile users' experiences, data management, integrated IT systems, and the speed with which data can be collected, analyzed, and utilized. Robert Leonhard in the book *The Art of Maneuver* writes on the role of tempo and speed, "If I can develop and pursue my plan to defeat you faster than you can execute your plan to defeat me, then your plan is unimportant." The words "faster than you can execute" in Leonhard's context refer to the tempo of operations.

In a fast changing world, mobile applications are competing for users and acceptance against the status quo (traditional paper or desktop processes) and competitors' apps. In order for organizations to be successful, they must deliver mobile applications that will meet the expectations of mobile users. A key component of a good mobile user experience, as we previously identified, is the speed with which it can load and respond to clicks, swipes, taps, commands, and queries. When asked in a survey how significant speed is to a user's overall mobile application experience, 80 percent answered "very important."[1]

Contextually Relevant Mobile Apps

It is well known that the more personalized and contextually relevant a mobile application or website is to the user, the more successful it will be at delivering a good user experience. Mobile apps and websites by their very nature are used on the move. That means the context in which a mobile device is being used changes rapidly. This data can be about locations, time, activities, history, and behaviors. This important data must quickly be collected, analyzed, and consumed by the mobile application fast enough to personalize the user's experience before the context changes. Cognizant's Center for the Future of Work calls this Code Halos.[3] This refers to all the data about a person, object, or organization that can be used to personalize and contextualize a mobile and digital experience.

The data required to personalize and contextualize an experience takes time to process and utilize. It often requires many different integrated IT systems. It needs to be captured, transmitted, analyzed, and shared in real time with the mobile application and used to personalize the user experience. The speed with which all of these steps can be executed is important. No matter how great a mobile application's design, delays in retrieving or interacting with back-office business or IT systems equate to negative user experiences. This is true for business-to-business, business-to-employee,

or business-to-consumer mobile applications. In order to be successful, IT systems must operate at speeds quick enough to satisfy all of these different categories of mobile users. This requires a serious review of every IT, operational, and business process component that ultimately impacts the speed of mobile applications.

The Shelf Life of Data and Speed

Today enterprises are facing a massive challenge that will require new strategies and investment. In fact, 80 percent of survey participants reported that increasing demand for mobile apps is forcing IT departments to rethink and change how they have designed IT environments.[1] Rethinking and changing IT environments requires investment and budget, and 83 percent believe the demand for mobile applications will force enterprises to make major investments in their IT environments to better support real-time interactions with mobile apps and to remain competitive.

We have determined that real-time mobile data is critical for personalizing and optimizing the mobile user's experience and promoting the adoption and utilization of mobile applications and websites. We have also determined that organizations, IT environments, and business processes will require changes in order to support a faster operational tempo. One of the key reasons these changes are necessary is the shelf life of data. Data has greater economic value the faster it can be collected, transmitted, analyzed, consumed, and utilized. This brings us back to the speed requirement. If the mobile user can instantly be presented with a personalized and contextually relevant experience based on real-time and previously collected and analyzed data, then the user will realize the greatest value and utility.

Situational Awareness and Information Advantages

Military strategists today believe the size of opponents and their weapons platforms is less representative of military power than the quality of their sensors systems, mobile communication links, and their ability to utilize information to their advantage. We believe these same conclusions are also relevant in the commercial sector.

An enterprise's ability to use information as a competitive advantage is central to a successful business strategy today. If a manager has the responsibility of optimizing the schedules of 5,000 service technicians during an ice storm, or routing 10,000 delivery trucks, then the faster they receive accurate data from the field and the better they can perform their jobs.

Information advantages often involve improving situational awareness — the ability to understand events and actions around you. This takes visibility and data. Visibility happens when people, mobile, and sensor data collection technologies are integrated with IT systems and processes that enable the measurement, collection, transmission, analysis, and reporting of remote activities and events. The faster this can be accomplished, the faster data-driven decisions can be made and tactics deployed.

Historically, it has been difficult to manage remote workforces due to a lack of visibility. There are too many unknowns and a lack of accountability, which forces managers to make decisions based upon conjecture, rather than on real-time data analysis. Robert L. Bateman writes in his book *Digital War,* "The three questions that have befuddled soldiers since the beginning of human history are: 1) Where am I? 2) Where are my buddies? 3) Where is the enemy?" Bateman speaks to the difficulty of managing from afar. The lack of real-time visibility often means critical operational decisions and optimized scheduling choices are delayed, which results in the inefficient utilization of resources and assets. Today technologies exist to eliminate many of those operational blind spots.

Network-Centric Operations and Data Collection

> *"Technology [used between WWI and WWII] was viewed in discrete packets as it applied to narrowly defined areas. As a result the US did not fully develop the possible combinations of technology with tactics."*
> –Robert L. Bateman, *Digital War*

Many commercial organizations today retain the narrow view and strategy that Bateman wrote about. They

continue to think about and deploy mobile and sensor technologies in line-of-business (LOB) silos. They believe in the utility of these technologies, but have no enterprise-wide strategy for combining mobile and sensor technologies with tactics to achieve an overall information advantage across the enterprise.

Modern militaries use the term Network Centric Warfare strategies to describe an information-based strategy for winning wars. These strategies have been taught in military organizations for decades, but are less understood in the commercial sector, where these strategies can be found with names such as Network Centric Operations or Networked Field Services. Military organizations that have implemented Network Centric strategies are accustomed to using a wide range of mobile devices and sensors to create a web or grid of data collection capabilities that are all wirelessly networked together for the purpose of enhancing real-time situational awareness, organizational agility, collaboration, and decision-making. Commercial enterprises share many of the same requirements, but as our survey data shows, they have yet to adopt the necessary enterprise-wide strategies or IT systems with enough speed to support real-time interactions.

Given the importance of an information advantage, what should commercial organizations focus on in 2015 and beyond? Broadly the answers are:

- Recognizing that information can be used as a competitive advantage
- Recognizing the importance of achieving real-time operational tempos
- Developing and implementing enterprise-wide network centric operational strategies
- Utilizing mobile applications and sensors to reduce operational blind spots and improve situational awareness
- Personalizing and contextualizing the mobile user experience using real-time data and Code Halos strategies
- Employing artificial intelligence and machine learning to improve the speed of decision-making and the execution of tactics

An organization's ability to be competitive now and in the future largely depends on its ability to successfully navigate the process of digital and organizational transformation to achieve an information advantage.

Kevin Benedict *is the opinionated Senior Analyst for Digital Transformation and Mobility at Cognizant and a popular technology pundit with more than 30 years of experience. He is a world traveler, keynote speaker, and writer on mobile, IoT, and digital transformation strategies and brings a unique perspective as a veteran industry executive who has taught workshops in 17 different countries over the past three years. Benedict authors the popular blog www.mobileenterprisestrategies.com. He wrote the foreword to SAP Press' book, "Mobilizing Your Enterprise with SAP," and has published more than 3,000 articles and numerous industry and analyst reports.*

REFERENCES

[1] The *Real-Time Mobile Infrastructure Survey* was conducted on www.mobileenterprisestrategies.com and included 80 IT and business professionals from across the world.
[2] Harris Poll of U.S. owners of smartphones and tablets.
[3] Malcolm Frank, Paul Roehrig and Benjamin Pring. *Code Halos, How the Digital Live of People, Things and Organizations are Changing the Rules of Business*. Hoboken, New Jersey: John Wiley & Sons, Inc. 2014.

Situational Awareness and Interoperability Defining Next-Generation Public Safety Mobile Solutions

By David Krebs

The changing face of public safety — especially in response to increased needs for agile emergency response and cross-agency communications — demands improved mobile communications and computing solutions. Mobile applications and wireless data services are increasing the opportunity for enhanced public safety response, improved coordination, and emergency communications. The need for dispatching centers to integrate text messaging and multimedia messaging services for emergency communications and responder alerts is increasing as new forms of communications and social media permeate public safety services. Next-generation public safety solutions are providing broader cross-jurisdictional access to records systems; augmenting existing land mobile radio (LMR) systems with interoperable broadband wireless systems for voice, video, and data; and extending data connectivity to all first responders across all patrol types.

Does FirstNet Answer Public Safety Communication Concerns?

A pervasive theme bearing on today's public safety solutions is the need for interoperable communications, especially as multiple first responder organizations collaborate. The Middle Class Tax Relief and Job Creation Act of 2012, signed into law in February 2012, included a section that opened the door to the First Responder Network Authority (FirstNet). The FirstNet plan is to build a broadband network for police, firefighters, emergency medical service professionals, and other public safety officials. The initial plan is for FirstNet to work with state, local, and tribal governments, with a goal to eventually create an interoperable, cohesive, country-wide network (though a provision allows individual states to opt out).

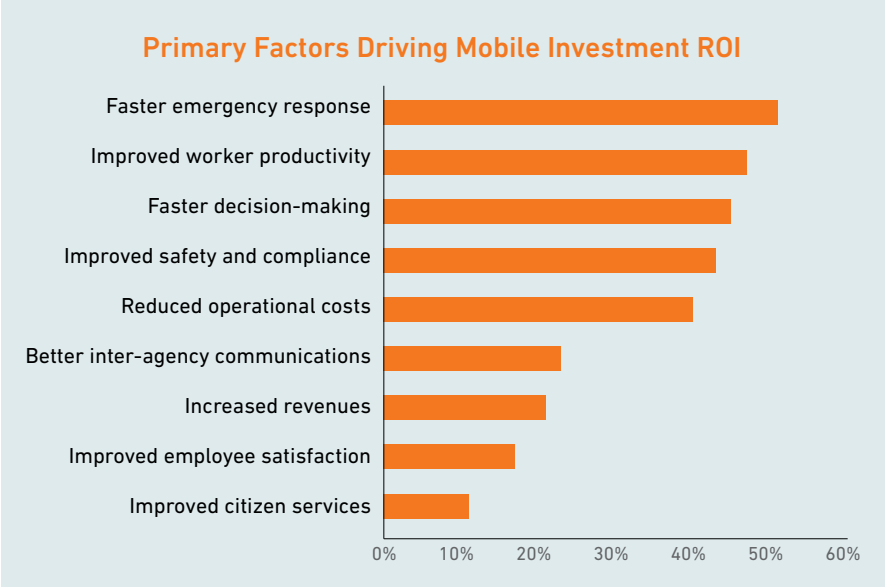
However, there is significant controversy surrounding the build-out of this network, especially regarding its financial viability. The system is estimated to be five to six years away from its first beneficial use, and existing radio systems will likely be in use for the next 20 to 25 years. One of the key issues will be aligning the subscriber fees (and potential total user base) with the significant costs associated with building out the

network. Despite all of the unresolved issues, this is conceptually one of the biggest advances in the history of public safety communications.

Proliferation of Mobile Apps Changing Public Safety

Public safety agencies will primarily continue to develop or purchase mobile device applications to support two primary functions:

- **Field Worker Support:** Police officers, first responders, and other mission-critical workers all desire to work more easily and efficiently. The ability to access and enter data from mobile devices will continue to grow to support these types of workers.
- **Citizen Interactions:** The public wants to be able to interact with government agencies via mobile phones and tablets. From communicating directly with law enforcement to various citizen services, the benefits of mobile citizen applications are far-reaching.



Primary factors driving mobile investment ROI.[1]

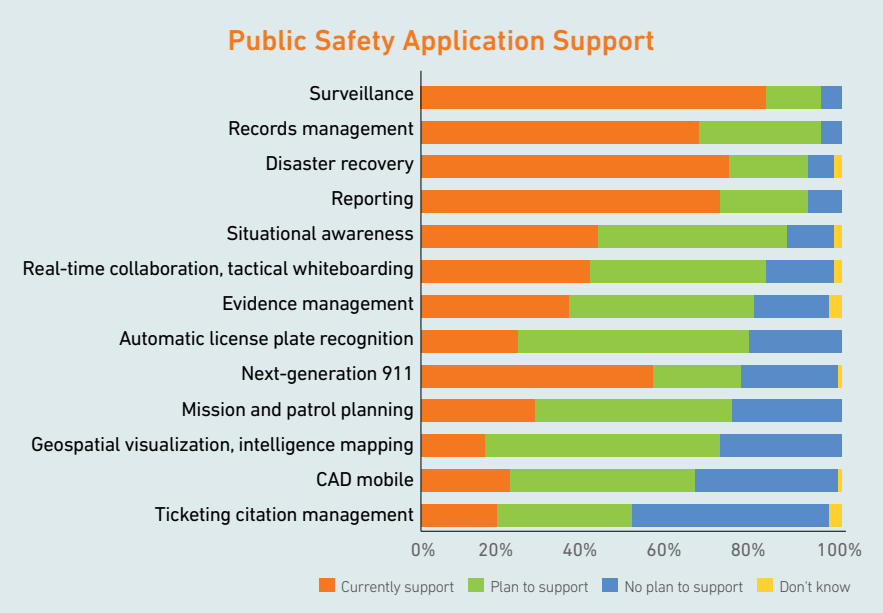
The current generation of government mobile applications is data-centric and allows users to interact with data residing in databases from mobile devices. What is lacking in many of these applications is the ability to interact with content such as documents, images, voice, and video content. Fundamentally, the need for first responders to react faster and improve in-field decision-making capabilities is driving mobile public safety investments. Providing access to richer content that can enhance situational awareness and enable greater collaboration among the workforce are critical enablers of next-generation solutions. Public safety agencies are starting to take advantage of advances in predictive analytics and collaboration technologies that foster the employment of more predictive and preemptive approaches to situation resolution and away from primarily reactive responses to crimes.

Mobile applications and wireless data services are increasing the opportunity for enhanced public safety response, improved coordination, and emergency communications. Of critical importance is the ability for greater intra- and inter-agency communications to provide the level of coordination required during significant events. In addition, communication between agencies and citizens is being enhanced, especially through the rollout of next-generation 911 services. These solutions are designed to enhance the 911 system to create a faster, more flexible, and scalable system that leverages communication technology used by the public, including text messaging and sharing of images, photographs, and other information seamlessly over an IP network.

The increased use of video and high-resolution imaging information for a variety of applications — such as disaster response — is evident. For example, during the Deepwater Horizon oil spill in the Gulf of Mexico in 2010, NGA support included analysis, unclassified commercial satellite imagery, and geospatial intelligence products of the Mississippi Delta and surrounding Gulf Coast areas. The products include imagery of major infrastructure along the Gulf coast, operational planning map atlases, and imagery depicting the extent of the oil spill. These types of products greatly assisted the U.S. Coast Guard in leveraging every available resource to respond to the Gulf oil spill. Some personnel deployed with the agency's Domestic Mobile Integrated Geospatial-Intelligence System (DMIGS) — a self-contained vehicle custom built on a fire truck chassis that allows NGA analysts to drive to a location and provide on-the-spot geospatial intelligence analysis and products.

In-Vehicle Solutions: A Critical Public Safety Integration Point

With more information to process and complex user interfaces to manage, staying focused on what's critical can be a challenge, particularly in the patrol vehicle. Officers need real-time information and intuitive, integrated vehicle controls — systems that



Public safety applications currently supported and planned to support.[1]

augment their senses and help them stay safer. While police cruisers are becoming smaller, there are more technology choices to deploy, such as automatic license plate recognition (ALPR) and real-time wireless video sharing, which pose an integration challenge.

However, advances in camera and video recording equipment have many law enforcement implications as well. Public safety professionals are documenting citizen interactions, vehicle collisions, witness interviews, crime scenes, and more with sophisticated, higher resolution equipment. ALPR software captures vehicle license and tag data at high speeds, providing valuable information that drives enforcement decisions. According to VDC Research, 40 percent of public safety agencies currently have in-vehicle technologies deployed, with another 34 percent planning on rolling out the technology. Similarly, approximately 60 percent of public safety organizations are currently streaming or planning to stream video content wirelessly to their police vehicles.

In-vehicle cameras document activities of police performing vehicle stops, and wearable cameras offer a more comprehensive view into all officer-citizen interactions. These new image-capturing technologies generate increasing amounts of digital evidence, which has to be well organized and accessible for court cases, news releases, and other uses. This complex environment explains the rise in digital evidence management solutions. Digital video and distributed sensor networks are playing increasingly important roles in vehicles for surveillance (e.g., collecting evidence, license plate recognition) and in video integration and access to streaming video content for operations.

Although public safety organizations are treating Computer Aided Dispatch (CAD) as their most important asset, departments are continuously seeking possible improvements for their CAD solutions in order to get the right information to the right place at the right time to improve real-time decision-making capabilities. Interest in next-generation public safety solutions — especially integrated evidence collection and situational awareness solutions — continues to grow; however, investment to date has been sporadic. Adoption cost and lack of standardized solutions remain key barriers. With the improvements in technology, the appetite for solutions using geographical improvements (i.e., AVL, GIS, GPS, and mapping software) is constantly increasing.

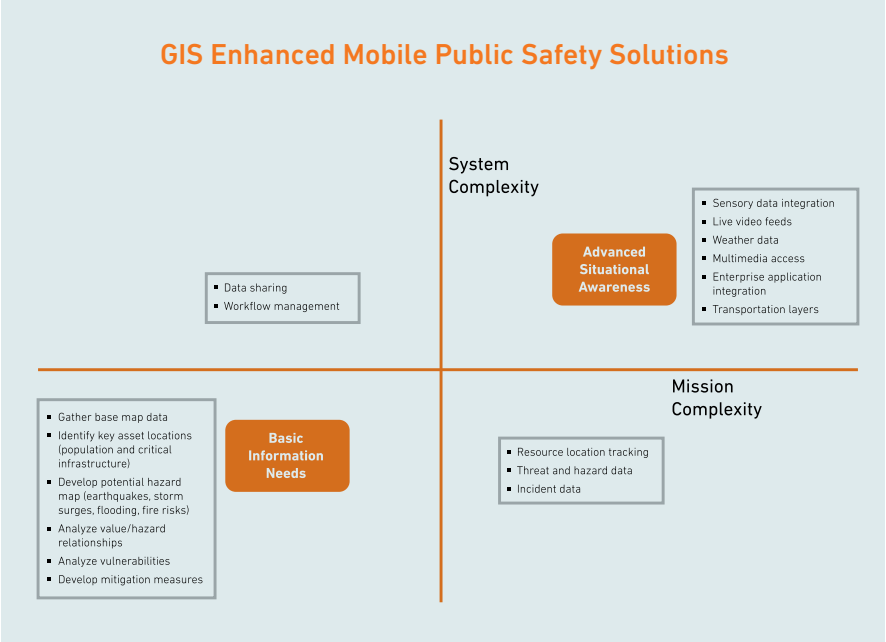
Despite security and privacy concerns, departments are more welcoming to both internal and external communication and collaboration tools. VDC estimates that the demand for these tools will increase in the upcoming years. LTE will enable higher quality video relative to existing 4G wireless networks. In most cases, public safety agencies don't currently support 4G solutions. Thus, LTE represents a major disruptive leap forward.

GIS Solutions Foundational for Next-Generation Mobile Public Safety Solutions

Mobile GIS is the expansion of GIS technology from the office into the field. A mobile GIS enables field-based personnel to capture, store, update, manipulate, analyze, and display geographic information. Mobile GIS solutions are considered critical enablers for improved field-based situational awareness. The advent of client-side web mapping technologies (e.g., OpenLayers, Google Maps, Bing Maps) has provided platforms for creating easy to use GIS mashup displays.

The competencies public safety organizations are seeking to create include providing access to relevant data in real time, integrating data sets into secure information bases, delivering critical insights to frontline public safety workers, and fundamentally improving strategic and tactical decision-making by better anticipating problems and directing the appropriate

resources to address them. In other words, complete situational awareness. Gathering and assimilating base information needs such as map data, asset locations, and assessment of potential hazard locations and overlaying real-time data feeds including weather data and video streams provides the advanced situational awareness required to make informed decisions.

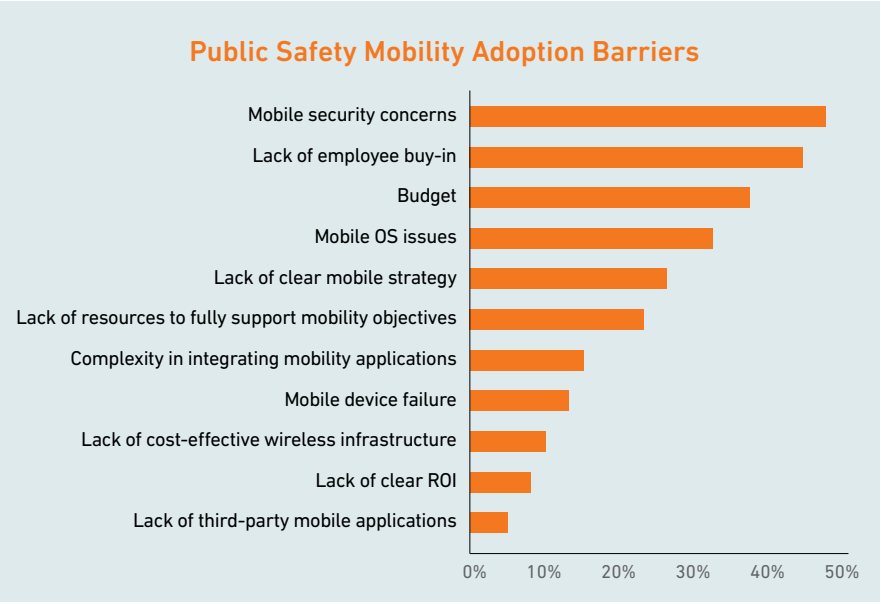


Security and Budget Concerns Leading Investment Barriers

The influx of mobile devices into public safety organizations is creating significant IT challenges from a management, security, and support perspective, particularly once organizations expand their mobile application range beyond de facto horizontal mobile apps like email, messaging, and calendars. Growing digital data regulations mean that organizations have to be sure they know exactly where their data is being stored, who is transferring it, and the level of encryption for all of their content. State and local government agencies require Federal Information Processing Standards (FIPS) 140-2 compliant solutions to protect their electronic data. FIPS 140-2 provides security requirements for cryptographic modules in mobile devices, making FIPS 140-2 compliant solutions critical for mobile security vendors. While many organizations are adopting more liberal Bring Your Own Device (BYOD) policies, highly regulated and security-sensitive customers will remain loyal to corporate-liable mobile policies due to federal mandates governing data handling.

While business leaders are increasingly aware of the opportunity presented by expanding access to critical business applications to mobile platforms, conforming to compliance requirements remains a high hurdle for organizations. Successfully managing risks requires cross-functional collaboration and the creation of policies and processes whereby security is a core element of the deployment plan. VDC advises companies to begin their mobile journey by ascertaining business goals, their expected cost savings, and revenue-generating opportunities from their mobile initiatives, as well as determining the level of risk they are willing to accept to achieve their goals.

Organizations must consider numerous factors when they evaluate and deploy mobile management solutions to address productivity and convenience while instituting mobile security policies that can help mitigate risks. The individual point solutions that were adequate for isolated mobile deployments are not sufficient in today's modern mobile enterprise. Ensuring the appropriate access to key enterprise resources such as email, databases, and line-of-business applications should be a top priority, as these are core to the central value proposition of a well-integrated mobile solution. Solutions should also be assessed to determine how



Public safety mobility adoption barriers.[1]

Providing access to richer content that can enhance situational awareness and enable greater collaboration among the workforce are critical enablers of next-generation solutions.

well they can integrate with existing authentication and access control mechanisms.

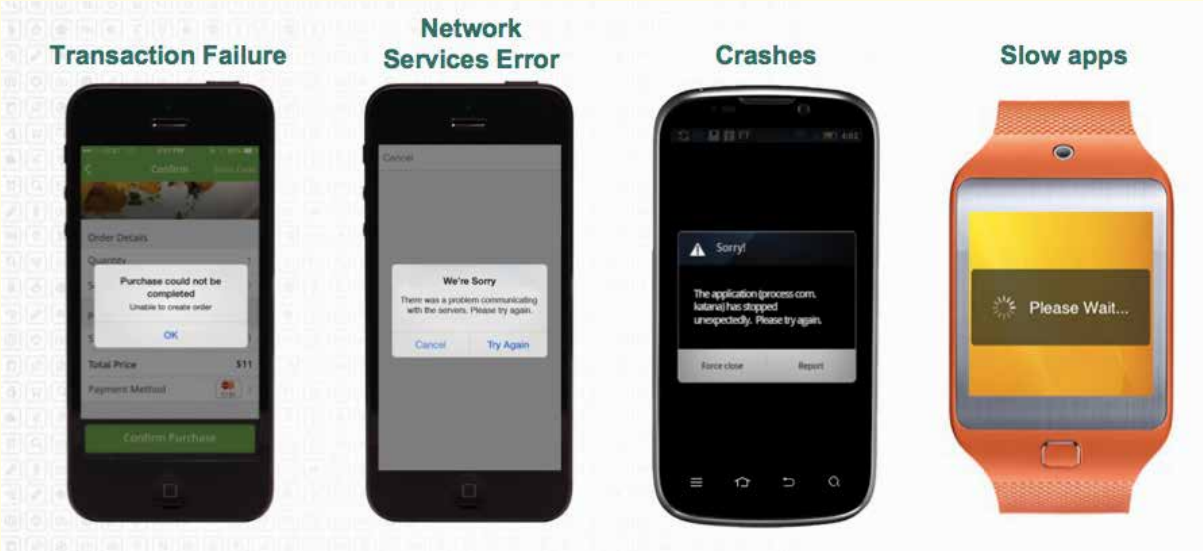
Device management will remain a cornerstone of security policy for mobile deployments. The ability to detect rooting or jail-breaking of the operating system, remote lockdown, and wiping of the device data, hardware feature controls, and remote control of the device are key features that are requisite to properly protect mobile assets and limit risk in case the device is lost or stolen. However, while satisfaction levels among those that have deployed an MDM solution are solid, organizations are finding that vanilla MDM solutions are not adequate for their expanding mobile deployment, particularly as their app usage becomes more sophisticated.

MDM's core features are requisite to properly protect mobile assets and limit risk in case a device is lost or stolen. However, organizations have come to recognize that they need to employ additional protections to ensure their devices and infrastructure are secure. The increasing risk of infection from malicious applications has made investing in solutions that offer real-time antivirus and malware scanning an important capability, along with the ability to identify vulnerabilities in web and mobile application source code. Context-aware detection and prevention capabilities are also increasingly important, as organizations are finding that they require secure access and authentication to a wider range of back-end services from multiple mobile apps and platforms.

David Krebs *is Executive Vice President for Enterprise Mobility & Connected Devices at VDC Research. He has more than 10 years of experience covering the markets for enterprise and government mobility solutions, wireless data communication technologies, and automatic data-capture research and consulting. Krebs focuses on identifying the key drivers and enablers in the adoption of mobile and wireless solutions among mobile workers in the extended enterprise and within government organizations. Krebs is a graduate of Boston University (BSBA).*

REFERENCES

[1] 2014 VDC Public Safety Decision Maker Survey



Apps are Now Mission-Critical

By Andrew Levy

As more business-critical functions move onto smartphones and tablets, a new approach must be taken to manage performance and user experience. Apps are a powerful way to drive innovation, collaboration, and a streamlined workflow for employees, but run on complicated, fragmented platforms that can be difficult to track — and the cost of failure is high. Apps are being used to track logistics and inventory, inside oil rigs to inspect parts and monitor pressure, by satellite technicians to repair service, and by healthcare professionals to diagnose patients.

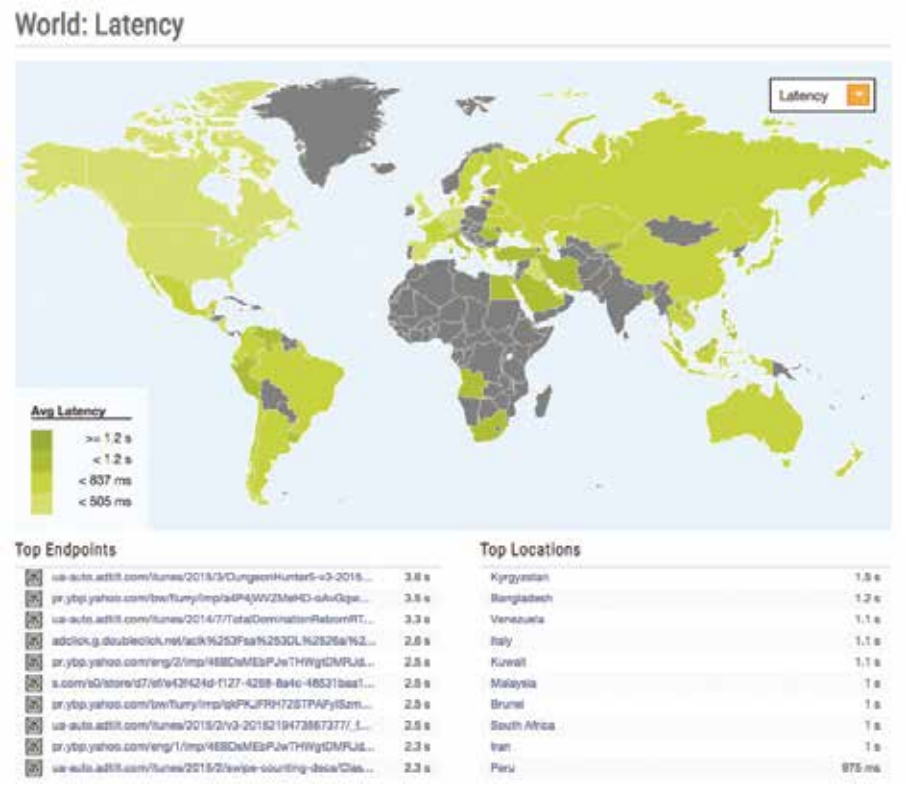
These are the kind of use cases where corrupt data, a confusing user experience, code defects, or failing hardware create both monetary and physical risks. It is more paramount than ever that organizations commit to understanding the various factors that can affect an app's performance in order to correct problems to prevent these situations.

Origin of Apps in the Enterprise

Consumer adoption and growth, along with commoditized hardware and software, have made personal smartphones and tablets ubiquitous in the workplace. In fact, 67 percent of Americans now own a smartphone, up from 35 percent just a few years ago, with a staggering 85 percent adoption rate among young adults.[1] This trend drove commercial and government entities to adopt Bring Your Own Device (BYOD) solutions such as mobile device management (MDM). These vendors typically allow companies to remotely configure, wipe, and secure smartphones. Now that enterprises have the tools they need to securely deploy custom mobile apps to their workforce, the dependency on those apps is increasing, but measures need to be taken to ensure the apps perform. As wearables and other connected devices enter the workforce, that task gains both significance and complexity. The Internet of Things (IoT) presents great efficiencies for organizations of all types, but a new set of factors will also affect app performance from traditional smartphones and tablets.

Why are Mobile Apps Different?

People tend to forget that mobile apps are really embedded software. They are highly dependent on the hardware and software configuration of the device.



Average latency by country.

iOS Crash Rates by Device

Device	Average Crash
iPhone 5	2.23%
iPhone 5S	1.96%
iPhone 4S	2.2%
iPhone 6	1.88%
iPhone 5C	1.92%

Android Crash Rates by Device

Device	Average Crash
SAMSUNG-SM-G900A	1.54%
Samsung Galaxy S5	2.06%
Samsung Galaxy S4	2.05%
SM-G900P	1.64%
Samsung Galaxy S III	1.78%

iOS and Android crash rates by device.

These embedded systems are more powerful than all of NASA in 1969, when we landed two men on the moon, and 12 times more powerful than the famous Deep Blue supercomputer from the late 1990s.[2] Complex offline calculations, location, various connectivity protocols, and powerful sensors are just a few of the differences versus the Web, which is still largely a client-server system.

Why Testing is Not Enough

There are a large amount of external forces that can impact mobile applications. The major forces to focus on include device, operating system (OS), carrier/Wi-Fi performance, cloud service problems, geographical issues, and code defects. These can lead to negative effects including device driver problems, operating systems deprecating functionality, carriers performing packet-shaping that corrupts data, cloud service providers unable to handle large data volumes, bandwidth issues in remote geographical locations, and poor memory handling by an app's source code.

Device fragmentation is often mentioned alongside Android, for which tens of thousands of different device types exist. However, there is OS fragmentation as well. iOS tends to release a point update almost once a month and those updates, although often intended to fix issues, can sometimes cause new problems for app maintainers.

Internal organizational politics and broken policies can also hinder mobile app performance. For example, mobile teams typically operate in a different department than other teams responsible for building APIs against internal systems. Mobile apps can often depend on a variety of internal and external APIs to function. A common problem occurs when those separate teams change the structure of the API, and suddenly the mobile team finds that the app is failing.

It is impossible to test every possible configuration, as there are hundreds of millions of permutations. Let's imagine an organization was able to test every possible scenario; as soon as a new device or operating system is released, a new app version is pushed to the device, or the app is used in a new locale, new bugs are inevitably introduced.

Key Mobile Performance Metrics

Regardless of the app's use case, it is important to track the right metrics; benchmarking and analyzing relevant data to make informed decision adds significantly to an organization's mobile strategy. There should be clearly defined goals for how mobile can impact the bottom line. Instead of focusing merely on user engagement metrics or business-specific metrics like transactional volume generated through an app, other mobile metrics should be considered:

- Proactively manage adoption rate — noting the specific device types and operating systems users are accessing the app on — to help provide a more detailed picture of user engagement.
- Monitor uptime by keeping track of crashes in real-time and determine if the issues can be solved immediately, or if the issue requires a new code push. Use analytics to find the root cause of the issue and if the error lies in the app's code or if an environmental issue (e.g., device, OS, or network) is at fault.
- Responsiveness, or how much faster or slower an app is running against its expectations, is a critical metric as a slow UX can drive users away. Connections, which can be further slowed by aggressive firewall rules or networks, are often the culprits here.
- Manage transactions by tying business metrics to performance data. Teams should optimize the most important transactions in the app — like account creation and login — and conduct root cause analysis by retracing user actions to see exactly where transactions are being disabled when issues occur, and which users are affected.

Recommended Approach

The first step in a holistic solution is to be able to triage customer experience, understand how many users are affected, and understand the business impact. For example, a bug preventing CRM entry into a mobile app might be prioritized above a bug impacting a mobile printing workflow. Once business impact is determined, a mobile manager can prioritize issues and assign them to the respective owner. The solution must help the organization discover who is at fault. For example, a failing third-party service provider might be assigned to an operations team for investigation, while a code defect is assigned to engineering, and a failing workflow in the app assigned to a product manager.

Sample metrics from Crittercism's mobile application performance management solution.

The next step is to undertake a root-cause analysis. This data should provide enough context for a team to recreate an issue in-house, or at the minimum provide enough data to a third-party service provider to implement a fix. If a third party is at fault, we often see an organization find a new or additional vendor, or alter usage from that provider. For example, a Salesforce API may provide unfettered access to customer records, but delivering too many to a mobile device may introduce latency problems. In this case, the app maintainer

Apps are a powerful way to drive innovation, collaboration, and a streamlined workflow for employees, but run on complicated, fragmented platforms that can be difficult to track — and the cost of failure is high.

may choose to change API usage to reduce data consumption, which also helps conserve battery life. If the issue can be fixed in-house, the solution should display the line of code at fault in the case of a code defect as well as relevant diagnostic data about the hardware and software configuration. User behavior should also be present to recreate the end user journey through the app — which buttons were tapped, what screens were viewed, and which network calls initiated eventually led to the issue.

Geographical performance is important as well, since an issue can occur anywhere in the world on a variety of connection types. These issues can be geopolitical in nature. Problems can also stem from physical landmarks, like steel bridges that block signals. A solution should provide enough geographical data to inform business decisions like selecting a carrier, or deploying additional content delivery networks.

The last step is to leverage analytics to trend app performance data over time. This is critical to measure the success of the organization's mobility initiative. The data should display the performance of each version of the application, and each platform configuration. These analytics can also help determine if a certain mobile operating system version or device type should be deprecated. The overall goal of the data is to demonstrate that the app is improving its performance from one release to the next. Q

Andrew Levy *is the co-founder of Crittercism, the leading mobile app performance provider installed on more than one billion devices. Prior to starting Crittercism, he was the co-founder of AdThrow, a Y Combinator company that built a data processing pipeline for real-time ad targeting. Before YC, Levy worked on data warehousing at HP Software. He has also worked for several companies in defense and intelligence, including Silicon Graphics Federal, Northrop Grumman, and Computer Sciences Corp. Levy has a B.S. in Computer Science from Johns Hopkins University.*

REFERENCES

[1] http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/
[2] Michio Kaku, Physics Of The Future: How Science Will Shape Human Destiny And Our Daily Lives By The Year 2100

The *IQT Quarterly* examines trends and advances in technology. IQT has made a number of investments in mobility solutions, and several companies in the IQT portfolio are garnering attention for their unique technologies.

BlueLine Grid

BlueLine Grid provides law enforcement, fire, EMT, first responders, and security teams with a secure mobile platform that allows them to find, communicate, and collaborate with each other regardless of jurisdiction or geography. IQT's investment in BlueLine Grid was recently covered by various publications including *VentureBeat*. BlueLine Grid became an IQT portfolio company in March 2015 and is located in New York.

MobileIron

MobileIron provides mobile enterprise management as an on-premises or cloud solution, purpose-built to secure and manage mobile apps, documents, and devices for global companies. MobileIron recently announced its AT&T Work Platform, which lets business customers add AT&T data, voice, and messaging services to their employees' personally-owned devices and keep personal service charges separate from corporate charges. This invoicing separation helps businesses overcome some of the administrative challenges to adopting Bring Your Own Device (BYOD) programs. MobileIron is based in Mountain View, Calif. and has been a part of the IQT portfolio since October 2012.

Mocana

Mocana provides a device-independent security platform that secures all aspects of mobile and smart connected devices, as well as the apps and services that run on them. Mocana has partnered with SAP to provide Mobile App Protection (MAP), which provides app-level security to pre-built SAP mobile apps, apps built using the company's mobile application development platform, and third-party apps. Mocana is based in San Francisco and joined the IQT portfolio in March 2012.

Tyfone

Tyfone provides software, hardware security, and payment products for mobile devices. The company recently launched the Fluide Mobile banking platform, which uses mobile app development and deployment technologies to bring secure and branded mobile banking apps to small and medium-sized community banks and credit unions. Tyfone became an IQT portfolio company in August 2012 and is located in Portland, Ore.

IQT
IN·Q·TEL