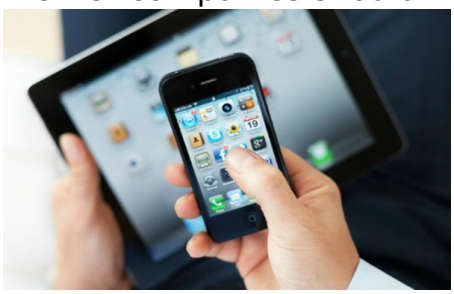
Why IT Departments Should Let Employees Use Their Own Devices

It's surprising to hear that there's still any debate as to whether companies should allow employees to use their personal mobile devices at



work. It's particularly perplexing when IT leaders are the ones who reject the idea. That's because the statistics are overwhelmingly on the side of bringing your own devices to work, also known as BYOD.

In a recent survey, 74% of IT workers [1]responded that BYOD is allowed in their workplace. Another survey found that 67% of North American iPad owners are using the devices in office, and IBM claims 80,000 BYOD users [2] in its fold. This is why CIOs and CTOs must be leaders in this movement, not barriers.

Being a leader means being prepared. IT has a great opportunity to help their business partners realize the productivity and cost benefits of BYOD while mitigating the new risks, most notably around security. Here are five steps that IT leaders can take to prepare for a positive BYOD transformation.

1. Innovate with Apps

Consumers have become accustomed to the purpose-built, highly-usable experience of their personal mobile devices and these preferences are carrying over into the workplace. This strong connection is fostered more by the mobile apps that they use than the physical device itself. The good news is that apps offer the greatest vehicle for business productivity gains and cost savings, but only if they are developed in the right way.

As with consumer apps, business mobile apps can and should be engineered to leverage the native capabilities of the device and to provide a rich user experience. For example, an auto insurance claims examiner who used to transcribe a claimant's statement on to paper, take photos of the vehicle, and have the claimant fill out various forms can now use a mobile app to record the claimant's testimony, photograph the vehicle and capture data with drop-down menus all through an integrated and digitized flow. This results in a faster and cheaper process, higher quality data, and more satisfied clients and employees.

It will be tempting for IT to simply uplift the existing user experience of current

business applications to the mobile context, but that approach would negate the potential benefits of enterprise apps. Companies like WillowTree Apps [3] and Taptera [4] offer good examples of enterprise apps built the right way. Enterprise IT leaders should follow this approach in order to realize the full BYOD opportunity.

2. Plan for Multi-Platform

One of the realities of BYOD is that there will be multiple device types and mobile platforms in the workplace. More importantly, as opposed to the web app world where browsers were viewed as commodities, there are enough differences between iOS, Android, Windows, and Blackberry to warrant consideration when developing mobile apps. In order to get the full potential out of apps, it is necessary to accept that not everything can be thin client. HTML5 is powerful, and will likely have more prominence in enterprise than it currently does in the consumer app space — where the platforms are competing outright.

The iPad is emerging as a unique business instrument with capabilities beyond what a smartphone can deliver, and its dominance of the tablet market warrants even more unique handling. As a result, there are apps that will be built only for the iPad, and that leverage functions only available on the iPad. In the insurance example, the claims examiner could collect the claimant's form data more easily with a tailored tablet app than with an app normalized for all mobile devices. IT leaders need to accept that platform-specific features are a reality in order to fulfill on the promise of enterprise mobility, but HTML5 and other common components can maximize development re-use and contain cost overruns.

3. Re-use Your Existing Logic and Data

The most fundamental way companies can maximize their investments in mobile apps is to build on top of the computing logic and data that already exists within the enterprise. Some mobile app developers have built their own back end applications and data repositories to service their apps, but this approach creates duplicate costs to run, maintain, and secure. A better approach is to open up the existing enterprise business logic and data through network-accessible Application Programming Interfaces (APIs). APIs have already been popularized on the mobile web used by consumer apps, through standards like REST and JSON.

In order to utilize consistent, customer-centric processing across all business channels, many companies moved towards a service-oriented architecture (SOA) in the last decade. This approach provides a solid foundation for enterprise mobile apps, but needs to be adapted to fit the lingua franca of the new paradigm. This can be done using an API Proxy that can map from SOAP to REST and XML to JSON, and also filter and cache data in order to limit the workload on the battery-operated mobile device.

Revisiting the insurance example, a big part of the productivity gain in having the claims examiner use the app remotely is that he or she can access their enterprise data in real-time. That means that they can have an up-to-the-minute view of the claim and the claimant, and also transmit the data they capture immediately to

headquarters. IT leaders who are able to harness their existing business logic and data will be able to deliver their enterprise mobile apps more quickly and save money doing so.

4. Secure the New Perimeter

Of course, given that the data in play for enterprise apps is often the most sensitive data in the company, security is paramount. Furthermore, given that the mobile devices in use for BYOD are personally-owned devices running a mix of personal and business apps, the API border that links mobile apps to corporate systems becomes the new security perimeter for the company. A blend of access control, data protection, and auditing is needed in order to protect the accessibility of the APIs.

OAuth [5] is the security standard of choice in mobile app-API integration. OAuth supports a number of use cases for authentication, authorization, and federated security, all packaged in a lightweight, token-based approach suitable for energy-conscious mobile devices. Just as for the data protocols, an API proxy can be used to adapt the OAuth protocols to the security policies and technologies that exist within the enterprise infrastructure.

Once secured, the APIs that serve the enterprise mobile apps become even more powerful. Many can be re-used for customer-facing apps. In the insurance example, the original claim could have been filed by the claimant using a smartphone app that included photos and digitized form data, through many of the same APIs that enable the claim examiner’s iPad app. IT leaders who implement flexible security for their APIs will position their company’s well for the benefits of enterprise and consumer mobility.

5. Embrace the Cloud

With a secure API perimeter that enables both consumer and enterprise mobile apps, companies are well-positioned to leverage the multitude of services that exist beyond their borders in the cloud. SaaS APIs can be combined with enterprise APIs to build a rich cloud platform for mobile app empowerment. The separation of concerns achieved through the secure API perimeter addresses the biggest risks associated with the cloud, data leakage, and unauthorized access.

In this scenario, the claimant who files the insurance claim can utilize their network operator’s geo-location API, or even the Google [6] maps API to capture precise location information regarding the claim, as can the claim examiner. This resulting ecosystem of highly usable mobile apps, accessible but secure enterprise APIs, and multi-dimensional cloud services creates a technological canvass for innovative IT leaders to advance their companies immediately and well into the future.

www.mashable.com [7]

Posted by Janine E. Mooney, Editor

May 15, 2012

Source URL (retrieved on *03/12/2014 - 5:48am*):
http://www.wirelessdesignmag.com/news/2012/05/why-it-departments-should-let-employees-use-their-own-devices?qt-digital_editions=0&qt-blogs=0

Links:
[1] http://www.techradar.com/news/world-of-tech/roundup/a-flexible-workplace-equals-20-more-productivity-1078272
[2] http://www.infoworld.com/d/consumerization-of-it/how-ibm-manages-80000-bring-your-own-devices-189504
[3] http://www.willowtreeapps.com/
[4] http://www.taptera.com/
[5] http://mashable.com/follow/topics/oauth/
[6] http://mashable.com/category/google/
[7] http://www.mashable.com