Top 10 Challenges to Retail Supply-Chain Mobility

John Leabeater, Sr. Mobility Architect
Coca-Cola Bottler Investments Group

Below is my list of 10 primary field mobility pain points which I have struggled with in field deployed solutions involving a near real-time remote connection. This could also be viewed as a "Proposed 2017 Future State of Mobility" brief.

All need to be viewed in terms of quantifiable costs. The business will continue to ask, "Why should I spend $3,000 on a rugged device when I can get similar results by spending only $800?"

1. **Power**: Support for a 10-12 hour work day without the need to recharge the battery. Battery recharging seriously impacts productivity and TCO.
    a. **In-Vehicle Charging**: Generally discouraged due to greatly reduced battery life resulting from frequent charging, the cost of vehicle charging hardware, and ongoing maintenance and business inefficiencies due to the added intraday charging tasks. Users should not have to think about charging from the time they leave their home or branch. This should be maintained while using GPS, WAN, and Bluetooth radios with high screen visibility in bright sunlight.
    b. **Smart Battery Management**: OEMs need to provide a simple mechanism for determining battery life based on average battery usage over time and the length of the work day. This allows for self-managed batteries and greatly reduces annual battery refresh budgets. The user should know when he needs a new battery more so than a centralized mobile device management tool.
    c. **Process Change:** Users should be responsible for daily charging. When field device EOD charge levels approach low levels (user defined) order new batteries or have new battery spares kept at the branch. The end user must assume responsibility for this process change – not the IT department. Cost control is ultimately a user defined behavior change.
    d. **Battery Embedding.** Retail computers ostensibly lower cost by embedding batteries. We typically assume a 2-year life cycle. So, if the battery is embedded into the computer will it provide an 8-hour service life after 6-7 days/week usage for 2 full years? If not then the user will become frustrated within days of first having to charge the battery before the end of the shift – and ask for a replacement that has better battery life.
2. **Communication**: Without reliable, secure communication to our backend systems automated data collection in the field is impractical. Communication must assume the following:
    a. **Reduce Dependence**: 24/7/365 cellular service cannot be assumed. Cellular networks can go down for weeks at a time in certain geographies under certain conditions (e.g. WV mining disaster 4/2009). Satellite solutions have yet to demonstrate cost effectiveness.

b. **Cellular Backup**: Redundant communication options via GOBI and Wi-Fi hotspot usage utilizing 2-tier authentication for VPN use must be included.
    1. Communication for field employees should include plans for protracted use of only Hotspot connections in the event of local communication downtime events.
    2. Programmatic profile selection must ease the burden of using VPN tools.
    3. Centralized control of GOBI WAN providers is preferred.

c. **Cellular Testing**: Cellular radio architecture must be *objectively tested* to insure the widest geographical coverage with the highest amount of throughput possible. Panasonic is one of the few OEMs with these rigorous standards.

d. **User Training**: Many users do not understand basic radio operation. Differences in the types of connections (Wi-Fi, Cellular, Bluetooth) and the connection process (radio state > tower association > authentication > synchronization) must be understood. Impediments to radio use such as geographic, atmospheric, configuration changes, and tower saturation should also be communicated.

e. **Reduce Bandwidth**: Pushing 7-32MB of data to remote locations puts a large strain on end users. Serious consideration must be given to data wants versus needs and the extensive use of data compression methods.

f. **Security**: Security is seated in the communication layer. Mobile solutions must utilize or be compatible with standard security mechanisms.
    1. **Active Directory:** Incorporates physical security requirements.
    2. **Virtual Private Networks:** Incorporates device authentication and encryption. We use Cisco AnyConnect for many field workers.
    3. **Secure Socket Layers:** For use in financial or intellectual property transactions. Cisco tends to be particular about SSL versioning.
    4. **Firewalls:** compatibility with our firewall architectures.
    5. **Device Authentication & Encryption:** support for Microsoft and Cisco infrastructure and security protocols.
    6. **Certificate Compatibility:** We currently use PRF files but would need the flexibility to adopt other types of certificates.

3. **Adoption**: Many individual users and business managers do not readily adopt mobile technology.

    a. **Use Case**: Incorrect matching of the use case to the solution causes low adoption rates. Poor battery performance, spotty radio connections, and a plethora of user options on a small screen greatly reduce the effectiveness and efficiency of the solution.

    b. **Process Changes**: The business struggles with *anything* that changes their process. They want newer technology *without* changing their processes. But a device change without a process change results in a very expensive solution.

    c. **User Profiles:** Users struggle with interfaces and work flows which assume familiarity with technology. Our user base generally falls into one of three categories:
        1. **20% are Efficient:** Users needs little or no help with field mobile technology.

    2. **40% are Average:** Users who require assistance with tasks such as changing passwords, communication options, non-intuitive work flows, etc.
    3. **40% are challenged:** Users who make technology work for them rather than using technology the way it was designed. These users will leave the mobile device in the car and work from "paper and pencil" using the device only when they must. Part of the solution for this group is the need for a "Yes" or "No" UI.
    4. **Fickle Factor.** Requirements should guide the platform decision, but users want what they want – and they are not sure what that is, especially once they use a device for a few days or weeks; i.e. they change their mind.
4. **Education**: Setting expectations and providing adequate training are keys to insuring adoption and usage. While a 3-5 year device life is a standard for durable form factors, nevertheless, it is not practical to reeducate users using the current 18-month consumer device refresh cycle. We need better ways to bring users up to speed more quickly.
5. **Ergonomics/Carriage**: the task, environment, and user profile should support a highly mobile field *worker* (vice administrator). *Reliability and durability are synonymous* and assumed. A solution will not provide assumed ROI unless the field worker will carry it with them for the task it was intended – particularly where hands-free usage is essential.
6. **Retail Life Cycles**: Assuming a retail device can be used in a field environment is precarious. Non-Intel retail device cycles rotate every 18 months – some sooner. This is very difficult from a logistics perspective (parts, device testing, etc.) and should be avoided if possible. However, one of the effective ways a retail device can be utilized is to:
    a. **Personalize:** Allow the user to use the same device for personal use: voice, data, SMS, MMS, etc. This significantly decreases the failure rate and greatly enhances user adoption.
    b. **Shared Cost:** Reduce enterprise costs by sharing the hardware and services cost. Among the most effective methods employed is providing the employee with a list of supported, corporate liable devices along with a payroll deduction for use of voice, data, SMS, and media services. This eliminates tax de minimis implications.
    c. **Managed Footprint**: Only a select number of devices can be allowed which are supported by the Mobile Device Management Server (e.g. WM, Droid, iOS). Non-enterprise support for the device and software is assumed by the user.
    d. **Policy Enforcement**: A formalized use policy where the device is maintained for work, rights are distinguished from privileges and where corporate interests are protected is essential. A mechanism for annual acknowledgement requirements must also be implemented.
    e. **Maintenance**: Thought part of the Shared Cost concept I emphasize that users must bear the lion's share of care for the device. What they break they fix or replace. When this is done failure rates plummet and efficiencies increase.

7. **Strong Browser**: It is very cost effective to run many management routines and LOB applications from a browser. The browser must be strongly supported on the client device. But many legacy enterprise mobile platforms have poor support for the browser.
    a. **Connection Problem:** The browser nearly always assumes a constant data connection. This cannot be assumed in many rural, coastal, and mountainous areas.
    b. **Solution:** Software development must move to an abstracted layer that is OS agnostic, runs in a disconnected state, and is supported by the hardware OEM. Motorola, via their Neon framework, is one of the few OEMs leading in this area.
8. **Extensibility**: Siloed devices increase cost, reduce functionality, and task support resources. It is difficult to allow promote this extensibility because large enterprise businesses are risk-averse. That is, they do not want to change anything about a process that is working.
    a. **Software:** Devices should allow for more than one type of application and use case where possible. This also allows for a single device platform being able to be used for multiple business applications so that a sales person's device could be used by a field technician and vice-versa.
    b. **Hardware**: "Snap-On" extensibility is not recommended. Modular extensibility is strongly preferred.
9. **Asset Management**: Ability to inventory and measure device performance is essential. The problem here is with spares and other devices that sit in a drawer for longer periods of time and devices, such as mobile printers, which have limited capacity for remote management. Even with MDM we still have a large number of devices which we cannot account for.
10. **Scope Creep**: We often build a solution with specific functions. But over time the business requires enhancements to that solution which fundamentally challenge the original choice of solution platforms. Therefore an OS agnostic software development platform greatly aids in resolving this problem. The following requirements for this platform are in view.
    a. **Multiple OS/Screen Sizes.** On multiple screen sizes and OSs: e.g. iPad, Blackberry, Android, and Windows (WP7, Embedded Handheld, and Win7).
    b. **Mobile Application Development Focus**. Some tools are all over the board. We prefer a focused platform that align with known skillsets or where the learning curve is short.
    c. **Rapid Development**: Time-To-Market is increasingly shortening. Ability to quickly deliver LOB applications is a requirement.
    d. **Compatibility to Standard Dev. Tools**: Development integration with Visual Studio Team Server 2008/10.
    e. **Compatible Synchronization**. We currently use a variety and would be interested in a compatibility, supplementation, or replacement approach.
    f. **Compatible to Backend Data**. Predominantly SAP, MS SQL, Oracle, DB2, SharePoint, ADO, ODBC, IIS, and cloud.
    g. **Cost Efficiency**. Cost efficiency/user is a key issue. We could use our MEAP (Syclo Agentry) for small user populations, but it is not cost effective to do so. We are

looking for an alternative which does not require a high licensing cost and consulting services to build.

h. **Remote Provisioning**. Support for a wide geographical user base (ability to remote provision using AirWatch).
i. **Disconnected Use**. Ability to continue collecting data in a disconnected WAN state.
j. **Security Architecture**.
    1. **Active Directory:** Incorporates physical security requirements.
    2. **Virtual Private Networks:** Incorporates device authentication and encryption.
    3. **Secure Socket Layers:** For use in financial or intellectual property transactions.
    4. **Firewalls:** Network layer and packet filters, Application-layer, Proxies, and Network address translation are typically used.
    5. **Device Authentication & Encryption:** AD, SAP MAM/MI predominate.
    6. **Certificate Compatibility:** prf files are used on our some handhelds. Certificates are also used on Android and iOS**.**