
Enterprise Solutions Blackberrization

“Accessing Data When You Want, Where You Want, How You Want”

March 2009



TABLE OF CONTENTS

Introduction	1
Business Value of Blackberrization	2
Mobile strategy	3
Mobile Infrastructure Limitations.....	4
IT Architecture	4
Technology Evaluation Criteria.....	5
Mobile Device Management (MDM).....	8
Mobile Device Security	9
Return on Blackberrization Investment	12
Implementation Considerations	12
Conclusion	15
Appendix A	16
References	17

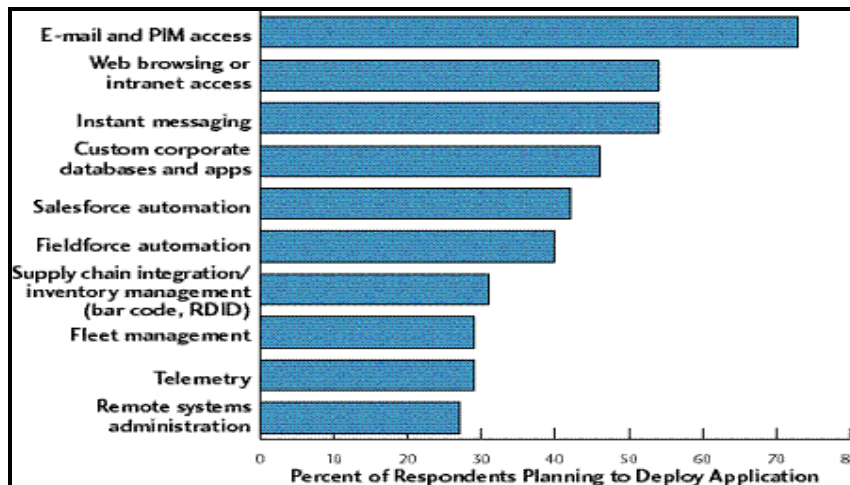
“Blackberrization”

Introduction

The action of moving business information and processes onto a mobile computing device, their use in the workplace and connecting them to an infrastructure has been referred to as “Blackberrization”. A term introduced by psychology professor Dr. Bryan E. Robinson Ph.D. in his 2007 book “Chained to the Desk: A Guidebook for Workaholics, Their Partners and Children, and the Clinicians who Treat Them” New York University Press.

The Blackberrization of business data and processes; allowing workers to access information 24 hours a day in a non-typical, virtual or outside of the office setting is a current reality that will continue to grow and mature in the coming years.

According to Interactive Data Corporation (IDC), a global provider of market intelligence for information technology and telecommunications; mobile workers accounted for 24% of the worldwide populations in 2006 and will account for 27% by 2009. This increase will result in a potential increase of 192 million mobile workers by the end of 2009 (Sudan & Drake, 2008). A 2006 study on planned mobility technology performed by the independent technology research and consulting firm Yankee Group, found that large U.S. businesses are embracing mobility in all aspects of business processing with the goals of increasing sales, worker productivity and improving service levels.



Source: [Yankee Group 2006 Transatlantic Wireless Business Survey--US Large Business](#)

“Just as the mobile phone progressed rapidly from dubious luxury to essential business tool, *so* mobile computing will become the norm for business.”(Computer Weekly, 2005). The coming revolution in the way information can be collected and disseminated, with standardized processes, will lead to improved customer satisfaction and increased sales for those companies poised to embrace the technology.

Business Value of Blackberrization

The potential benefits to a company deploying an enterprise mobile solution are obvious: reduces delay, enhances customer service, increases employee productivity and generates significant business efficiencies (Ambidge, 1999).

- The Children's Hospital at Westmead, Australia, observed dramatic improvements in staff productivity, potential cost savings and patient care by deploying a mobile wireless system in the Emergency Department. The department was able to save twenty hours of staff time per day, which equates to 7,439 hours per year. The assurance of a fast response rate increased from 38 % to 46%. This significant increase in response time is a direct result of doctors receiving an instant notification, increasing productivity and satisfaction with the way the technology supported clinical staff's delivery of care (Cisco, 2007).
- University of Connecticut Environmental Health & Safety (EH&S) achieved a 57% increase in the number of annual lab inspections performed by transforming a paper-based process to a mobile data collection process. The transformation allowed EH&S to eliminate redundant data entry and improve the quality of data and to easily access critical EPA and OSHA compliance reports (TISCOR, n.d.).
- Indian farmers utilize mobile technology to instantly receive valuable information pertaining to crop prices, weather forecasts and relevant agricultural news. Access to this current data helps farmers feel empowered in negotiations with suppliers and customers and results in increased direct financial returns (Flinders, 2009).
- In 1999, AMF Bowling Worldwide, Inc. (AMF) used data collected using a mobile sales force automation solution to target promotional mailings to prospective customers (500~1000 accounts). This strategy was used instead of sending mailings to 6000 of its nationwide accounts, resulting in 60% cost savings per promotion. The mobile automation solution enabled the sales representatives to update customer's equipment profile and enterprise database while visiting a customer location; the management team was able to make business decisions using the most current data. One successful promotion yielded \$601K in revenue, up from \$252K the prior year. (Dragoon, 2002).
- In 2000, Carlson Hotels extended its investment of over \$20 million in core reservations and information management by deploying a new wireless, portable information system called Mobile Access to Carlson Hospitality (MACH-1). The concept behind MACH-1 is to provide each manager with what they need to know, when they need it and have access wherever they happen to be, in real time. MACH-1 provides corporate executives, field support staff and sales people instant alerts based on triggers that can be set individually by each user. The real-time data notification translates into better customer service for guests and better financial results for the hotels (Hospitality.Net, 2000).

- IDC found that in Western Europe, small to medium-size businesses achieved a 22% increase in profitability as a result of adopting Internet technology solutions. The study showed that most of the increase in profitability could be attributed to the use of mobility access technologies and enabling devices and solutions (May, 2006).
- The International Telework Association and Council estimates that 50% to 70% of office space is unoccupied during normal business hours. Similarly Nemertes Research found that 87% of workers do not work at the company headquarters. Using a mobile solution can directly reduce the office space and associated expense required to support employees. (Sharpcomm.com, n.d.)

Based on the documented cases above and many other related statistics, it is clear that Blackberrization and enterprise mobility solutions can revolutionize the way a business operates and allows them to provide higher services levels to their customers. The ability to access or upload information from the point of customer contact empowers decision makers and helps track resources. These benefits provide all businesses with the opportunity to increase productivity and more effectively manage their operations.

The significant barriers to introducing this technology throughout the enterprise are primarily cost related, although additional consideration should be addressed in the areas of security, system infrastructure and enterprise wide strategic implications. In order to successfully deploy and support Blackberrization, a mobile strategy must be formulated to align the business processes and needs with IT processes.

Mobile strategy

With such positive impact on business productivity and service being reported, it is easy for businesses to assume this is the next big thing and deploy resources towards enhancing their mobile computing ability. Currently, there is a significant investment in deploying a mobile computing solution. As a result, it is necessary for businesses to assess which customers, processes and who within the organization will benefit the most from this investment.

When the Internet was first rolled out by businesses it became apparent that the ability to have a website did little for business growth or efficiencies. What added value to companies was offloading operational functions and providing data to customers at their convenience. The key considerations for mobile computing are to deploy the functionality where it will positively impact the business. The company must develop a mobile strategy that defines:

- “How, when and where to deploy mobility?
 - Which user groups need specific mobile devices, services and applications?
 - How mobile devices and services will be secured and managed?”
- (Johnson, 2007).

The organization should approach mobilization as a business project and develop strategies to support the defined needs, not a technology problem although there are clearly technical considerations (Sage, 2007). The limitations associated with mobile devices and the established corporate infrastructure must be addressed in the mobile strategy as it is used to support mobile technology.

Mobile Infrastructure Limitations

Connectivity Constraints

Good network connectivity is the backbone for a mobile application. Even though the majority of the U.S. has wireless network connectivity available, Service Providers still encounter dead spots or slow networks that can impact the performance of a mobile application, particularly when substantial interaction is required with back office systems.

Device Limitations

Users are accustomed to the fast performance of their desktop PC and they expect the same from their mobile devices. The small screen, difficult navigation and hardware (memory/processor/storage) constraints can lead to end user frustration and makes the deployment challenging considering the diversification of devices in the marketplace.

Data Storage and Synchronization

How much data and the number of applications that must reside on the device should be addressed, given the physical limitation of the device. Storing more information locally results in less reliance on the network and can compensate for poor connectivity, but may stress the device resources resulting in poor performance, end user frustration and potentially increases the risk of a data breach.

Business Process Extension

In order to support the mobile workforce, the business process workflow must be extended and optimized to fit the device and work requirements.

IT Architecture

Once the mobile strategy has been created it becomes the responsibility of the IT group and the business side project sponsor to deploy any mobility solutions. The areas of consideration for the IT group to assess when evaluating enterprise mobility solutions include determining the appropriate system infrastructure, and the technological comparison of various products. Additionally, mobile device management, asset management and device security should be evaluated to ensure that they meet the goals of the business needs and are aligned with the overall mobile strategy.

Technology Evaluation Criteria

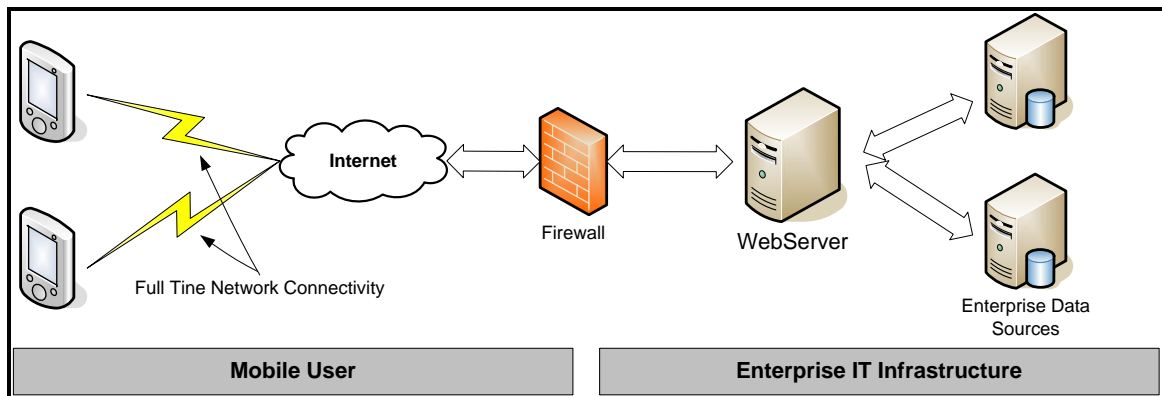
Besides addressing the limitations of the mobile infrastructure as defined in the mobile strategy, the IT plan should evaluate the business requirements in order to maximize the usability and functionality of the mobile solution. Some of the needs to be evaluated are:

Mobile Client Architecture

Will the mobile worker access the application as a browser-based application (*thin client*) or as a feature-rich local client application (*thick client*) or as a combination of both?

Thin Client

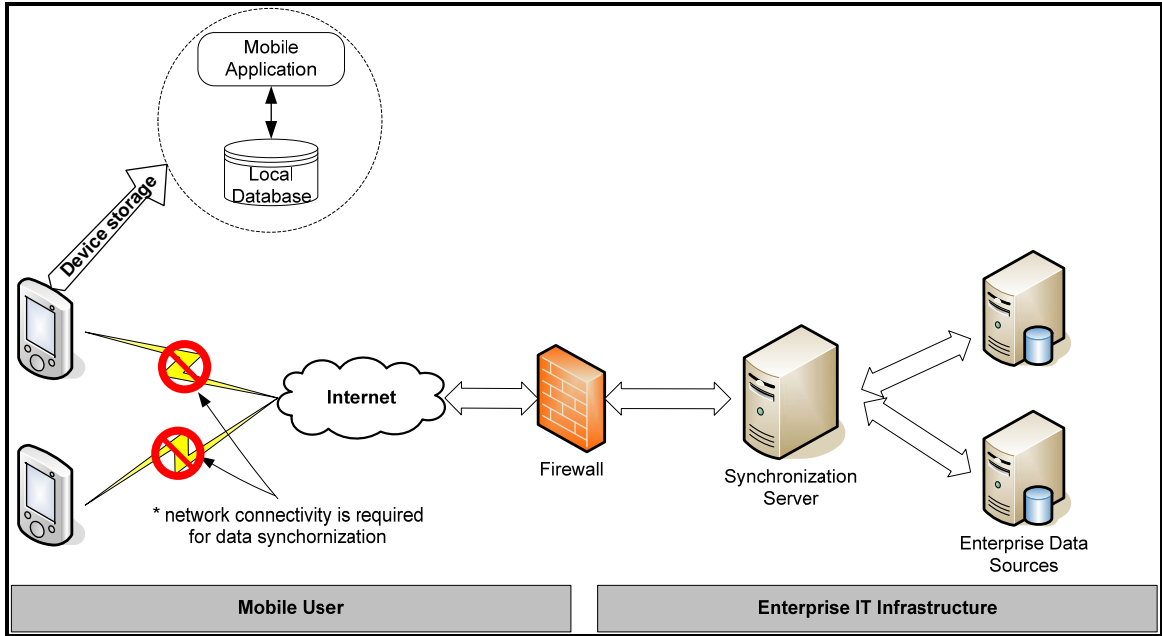
The solution is accessed through the browser on the device and does not involve deployment of any application or local data storage. It is typically easier to implement, manage and secure but requires full-time network connectivity for successful operation.



Thin Client Implementation

Thick Client

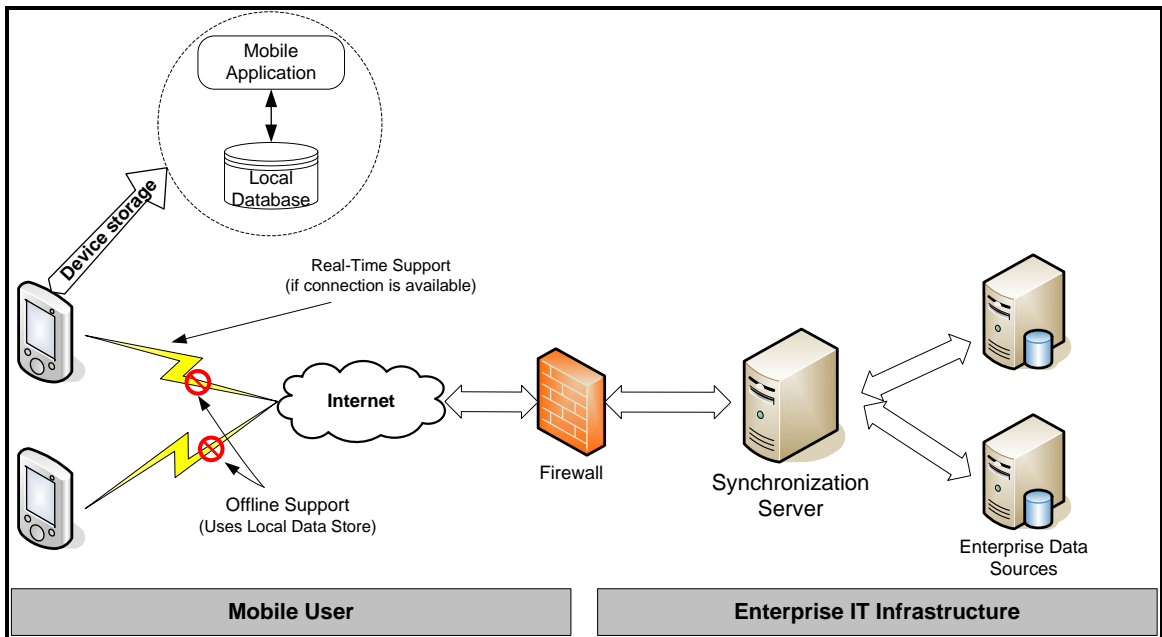
The solution and local data is deployed locally on each device. It requires significant development time and increases the complexity of device management and local device security but the user's productivity is not hampered by lack of network connectivity.



Thick Client Implementation

Smart Client

The best of both thin and thick client are incorporated into one hybrid architecture. In this architecture, the solution utilizes the network connectivity for real-time data access, when available and allows the user to work in offline mode when there is no connectivity.



Smart Client Implementation

In a Smart Client implementation strategy, there are many considerations and questions and concerns that should be addressed to insure a successful deployment and easy adoption by the users.

Data Delivery

- For client-based mobile application deployment, will the data be pushed to a user in an automated fashion or will the user manually pull down data to the device?
- Both the push and pull approach will rely on middleware components to facilitate the data exchange.

Off-the-Shelf or Internal Development

- Will the business deploy a mobile extension provided by the enterprise application vendor or will it be internally developed?
- Mobile extensions are easy to deploy and must be evaluated to ensure that it fits the business workflow. On the other hand internal development takes a long time to deploy, but the solution is mirrored to automate the business processes.

IT Infrastructure

- Will the mobile enterprise solution be deployed on a separate machine requiring its own set of server based components or will it be deployed on an existing mobile infrastructure?
- Deploying it on an existing infrastructure will result in faster turnaround time and lower cost, but the effect on performance by adding new solutions should be carefully evaluated.

Supported Device

- With the continuous diversification of devices, will the solution be deployed only on one type of device or does the solution need to be device agnostic (support multiple device type)?
- Will the devices be used in a typical office or work environment or do the devices need to perform in harsh and extreme conditions?
- Can the mobile worker perform their jobs on readily available consumer device (BlackBerry, iPhone, HP iPAQ) or do they need more durable, ruggedized industrial device (Motorola/Symbol, Intermec)?
- The mobile strategy deployment cost is significantly affected by the device type due to the big price variance between consumer and industrial mobile devices.

Connection Technologies

Security issues will need significant consideration and will impact decisions being made regarding connection technologies. Professionals must evaluate whether to use VPN to maximize security or utilize a connectivity path through a network operations center (NOC). The technology selected will be governed by what is already being utilized and what can be supported on the device selected.

Mobile Device Management (MDM)

Mobility allows an organization to experience increased productivity but needs to be effectively and efficiently managed. Proper controls must be implemented to mitigate the inherent risks of sensitive remote/disconnected data and applications (Sudan & Drake). Without proper tools, it is a daunting and challenging task to manage mobile devices connecting to the network as well as the applications and data on the device.

A good mobile device management solution has the ability to go beyond device management by giving IT the power to control applications and data (Oliver, 2008).

With the availability of numerous MDM tools in the marketplace, companies must ensure that all systems integrate efficiently. When selecting a MDM tool, IT professionals must consider whether the tool will successfully integrate with other processes (desktop or laptop management) that have been put in place to meet existing company policies and compliance mandates (Sudan).

Device Monitoring

“A top-notch mobile device management system simplifies routine management tasks by enabling regular monitoring of devices to ensure compliance with corporate policies” (Oliver). Since mobile devices are typically spread geographically and are dependent on network connectivity, it is often a challenge to manage and monitor the device to ensure compliance. A high-quality device management solution must react to changes in the actual device by monitoring files, folders, memory and registry settings. Management solutions will look for changes whenever the device is connected to the network. (SOTI.net, 2008).

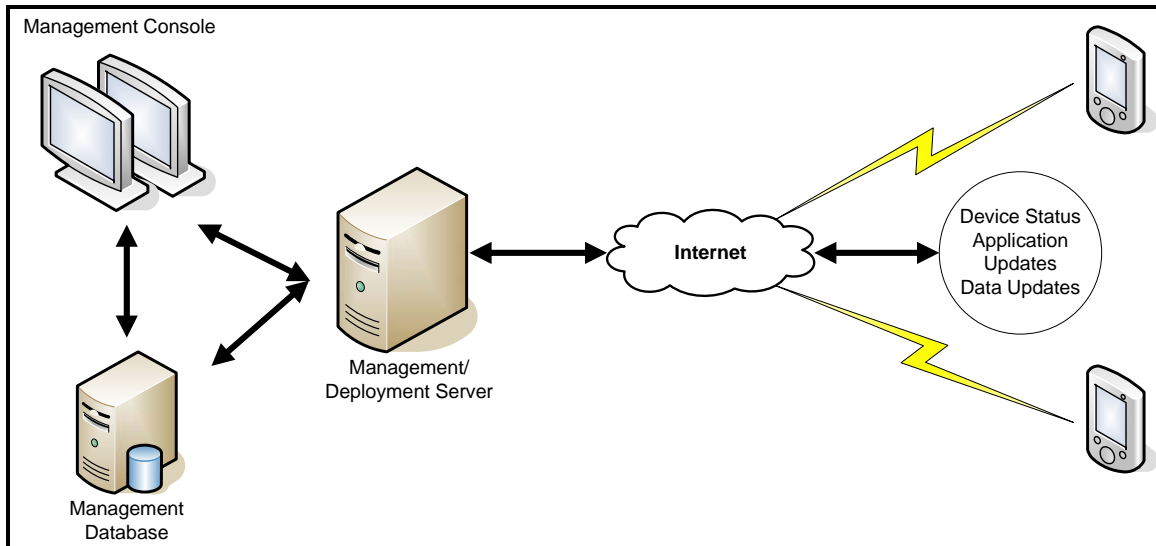
The device monitoring solution should also allow the IT support personnel to remotely login to the device to view exactly what the mobile worker sees in real time to troubleshoot the device. This results in a decrease in downtime and labor costs and contributes to a decreased total cost of ownership.

Asset Management

The mobile device management solution must provide visibility into frontline devices so IT managers know exactly what devices are deployed, where they're located, and what software is installed (Oliver). By deploying an MDM solution that includes asset management capabilities, businesses can ensure that licenses for mobile device growth is properly planned for and are properly managed (Sudan & Drake).

A device management solution typically consists of:

- *Management Console*: Application to manage policies and monitor devices.
- *Management Database*: Repository to store the mobile policies.
- *Management/Deployment Server*: Server application to push policies to the devices.



Device Management Solution

Mobile Device Security

Mobile devices present a unique set of challenges to IT security. As part of the strategy development, it is important that security issues are thoroughly reviewed and addressed to insure that data is not compromised, and the company is protected from any financial impact. Mobile devices have the same security challenges that any networked PC does plus some additional challenges, yet they are often treated less important than a laptop from a security standpoint. Handheld devices typically have the same capabilities of a laptop; therefore, security issues should be defined with that in mind. Being more mobile than even a laptop, mobile devices have an increased risk of being lost or stolen. Traditionally, palm type devices have software that, at least in some cases, has fewer and less robust built in safeguards than current PC software. These devices often have fewer updates and security patches available to correct or address security issues. With less capability to push software, they are less likely to be managed by IT security policies and policy enforcement. The variety of devices and platforms available can make centralized control difficult, especially with the limited availability of cross platform solutions. All these factors and more make mobile data device security a challenge to implement and enforce in an enterprise environment. These issues must be considered and challenges overcome when authoring and implementing a security policy for mobile devices.

When launching a mobile strategy with best practices in mind, mobile device deployment will be done methodically with clear goals and policies and employing applications the company requires.

In a worst-case scenario, IT is asked to bring order to a completely unregulated deployment of mobile devices with mixed hardware, software and ownership. Either way the process needs to start with a security policy so that financial and business impacts can

be assessed up front. While this security overview won't go through all the security steps in detail, the security policy should include or at least consider the following:

- Acknowledged acceptance of IT policy
- End user device retention
- Password authentication requirements
- Remote lock and wipe
- File Backup and Restore
- File Encryption
- Allowed/restricted applications/software
- Allowed data communication protocols
- Bluetooth control
- Data timed autodelete
- Logistics surrounding deployment/support
- Smartphone as a thin client only

Extension of a Corporate Security Policy

The first (and arguably the most important) step in a security policy is to require any mobile device that connects to a corporate network follow the same corporate security policies as any currently used desktops and laptops. Mobile devices are putting the same corporate network and data at risk (Sudan & Drake). This is especially critical for companies that allow end users to use a personal mobile device on the corporate network. Following the same corporate security policy with sets expectations of the end user gives management the information it needs to accurately estimate the cost and manpower required for the deployment of mobile solutions.

Physical Security

The keystone of protecting the data on a mobile device is physical security, from a policy enforcement standpoint; it's also the least controllable. The small form factor of the devices makes it much less likely to be missed as quickly as a laptop. They are easier to misplace, and are also a relatively easy target for a thief. A mobile security policy must stress the importance of maintaining ownership of the device to the user. The company must clearly communicate to its mobile devices using staff the importance of protecting access to the data that resides on the device and the potential impact to the corporate network security. In addition, physical upkeep should be provided and encouraged, including replacement of worn or broken cases and clips and issuing security tethers to mobile workers. As part of the strategy, IT professionals must devise a disaster plan to address the check list of tasked that must be followed when a device has been lost. A solid plan will minimize the impact on data loss or compromise.

Lock & Wipe

The ability to lock and wipe a lost or stolen device remotely might be critical if devices have sensitive files or email attachments. Ideally the process should be able to be initiated manually as well as being activated after a certain number of failed password attempts.

Data Security

The prevalence of removable SD memory cards for storing information means that setting a basic “wipe” policy is no longer adequate protection for corporate data – especially when the wipe delivery is not assured. Data needs to be protected at all times, including the interval that elapses before the loss / theft of a missing device is detected and reported to IT.

File Encryption

FIPS 140-2 validated AES 256-bit algorithms can be used to encrypt files and data for both on-board storage as well as removable storage cards. Encrypted data on a lost or stolen SD card cannot be read by an unauthorized device, thereby securing corporate data stored on a card. Real-time key escrow at the time of key generation provides an emergency recovery mechanism to retrieve data from SD cards in the event of hardware failure

Application

A list of allowed and denied software needs to be part of the policy as well. It does little good if IT designs a safe and secure software solution and the end user replaces it, in whole or in part, with software they prefer. If the user is free to download, add, delete software without notification, then the device is at risk of possibly disabling or bypass security.

Data Communication

Like a PC, a mobile device can be compromised if there is unauthorized access to the network or corporate data. It can also act as a back door into to enterprise network, allowing the introduction of malware or viruses to bypass the normal firewalls and virus scans. Data and voice travelling over wireless protocols can be intercepted. The implementation strategy should require full encryption of over-the-air transfer of data. To ensure added safety the strategy should also enforce VPN use, and unsafe protocols such as Bluetooth and Wi-Fi need to be disabled or controlled.

Support Policy

Mobile device security policy should define the logistics for deployment and support, for example:

- Will device repair and replacement be done in house or through the service provider?
- How will security be maintained if the service provider does a phone replacement?
- How will emergency support be handled?

Each mobile device OS has its own strengths and weaknesses. Whether a company decides on a single solution or a multi vendor solution, it is important to evaluate the capabilities and limitations of all devices. [Appendix A](#) describes the OS security limitations of several well known, consumer mobile devices available in the market place today.

In an ideal security environment, PDA security would be set up like PC security. Devices and software would be chosen and tested by corporate IT departments and issued on an as needed basis with clear policy, monitoring and oversight. This allows for maximum security with minimum complications.

Return on Blackberrization Investment

“Mobile technology is the fastest growing area of IT expenditure. By 2008 mobile enablement will be the second highest technology priority, according to Gartner, with business intelligence remaining number one and real-time enterprise support technology becoming the third highest technology priority for CIOs” (Computer Weekly, 2005). While articles extolling the virtues of mobile computing, illustrating many of the desired benefits, like improved customer service and increased worker productivity, these are not clearly measurable expense savings or revenues enhancements.

“Translating gut feel into hard cost savings or productivity gain into profit is not simple. New technology generates new performance indicators, which makes measuring success up-front difficult.” (Lion, 2004).

Any substantial investment, such as the one necessary for developing a system to support a mobile strategy, needs to be evaluated against the enhancements to revenues and expense savings. The mobile strategy must be closely scrutinized so that the supposed benefits are being correctly quantified. The current work processes needs to be measured in as many aspects as possible to create a base line which can be used to assess the results of a mobile device deployment. To do this thoroughly will require – time to collect data, evaluation of the amount of time it takes to complete the core job tasks, customer satisfaction levels, employee turnover rate, the hard costs associated with the entire process (all personnel including data entry personnel), amount of down time or other costs associated with errors (bad data entry, uninformed decisions, etc.); the same metrics should be measured every quarter for at least two quarters to track and assess the results allowing businesses to continuously improve the process (Dedo, 2004).

Implementation Considerations

Any enterprise wide technology solution that has the potential security and data risks paired with the business rewards, as a mobility solution, must be thoroughly planned out to mitigate risk and ensure a successful implementation. As identified earlier there are many factors to consider when deciding to deploy a mobility solution from IT architecture, business processes, security, types of devices, services to perform and which carrier to use, just to list a few. While a detailed implementation plan is beyond the scope of this document the following items should be taken into consideration when deploying an enterprise wide mobility solution:

Project Definition –

- Project Scope & Goals – Should be defined by a cross functional and organizational team comprised of business and IT staff. The project goals must align with overall business strategy
- Project Benefits – How will this project benefit the enterprise
 - What processes or services levels can be improved that will result in organizational gain
- Project ROI – Expected return on the overall project – what is expected in both measureable and non-measurable areas, should include both hard and soft costs
- Project Leadership – Define who the business side project sponsor is and who is the lead technology person

Project Team -

- Establish a formal project team with a defined charter and outlined team roles
 - Project sponsor responsibility should be defined
 - IT resources – How many are needed and will they be available when needed
 - Business resources - How many are needed and will they be available when needed
 - Will outside / consultant resources be needed

Technical Environment and Architecture

- Determine technology needs at handheld and required server levels to meet project scope and goals
 - Thin – thick or smart / hybrid client
 - Types of other infrastructure needs
 - ✓ Are dedicated servers or additional firewall security features required
 - What handheld device types are needed to meet deployment requirements, and meet user needs
 - Will new software be required for integration or is an off-the-shelf solution available - how will the mobility solution integrate into the business processes
- Which wireless carrier or services to use, type of plans and billing structures
- What type of connectivity is required to meet project objectives
 - Connectivity to the office (VPN or NOC)

Security

- Define required security functions and features
 - How to handle physical device security
 - Data transfer – how to secure information moving back and forth from the handheld to the back office – is file encryption required
 - How will the connectivity to back office applications and infrastructure be secured – will security features like additional firewalls be needed
 - How to handle other data security needs – memory cards
 - Wi-Fi –is this an item to address as there are potential security risks with having Wi-Fi enabled on devices that connect to back office systems

- Authentication and Identification – how to ensure that only authorized people have access to data and systems available from the mobile device

Device Management

- Device Monitoring – what is on the device, how is it being used, identify its current location and its configuration and evaluate the performance of the device
- Asset Management - how to track devices in use; what is on them, who has them and their location
 - Licensing
 - Installed applications and configuration
 - How to wipe / clean a lost device
 - Provisioning information of when they are issued and to who
 - Hardware and Software updates status – ongoing management to ensure all systems are at required operational levels
 - Monitoring of coverage and device utilization
 - Ordering and billing – review of billing to ensure costs are being monitored
 - Evaluation of Software and Hardware Maintenance plans to ensure features: specifically, functionality and security needs are being met

Pre-Deployment Testing

- Defined goals of testing – expected measurable data as a result of testing process
 - How to test and who tests before deployment
 - Identification of users for pilot phase
- Approval of testing – who has the authority to release the project for full roll-out

Training - On-Going Support – Other Items

- Who and when to train – who is responsible for training
 - When to repeat training – how often to train
 - Are there different levels of training depending on how the device is used
- On-Going Support (not addressed in Device Management)
 - Will there be a helpdesk to support users – how is the helpdesk trained
 - What is the availability of support staff – will there be after hours support for people in the field
- Conduct a post project implementation review to review outcomes of project

Formal Documentation, Policies and Procedures Needs

- Security, monitoring and device management – documentation, policies and procedures
 - How to wipe/secure a lost device policy and procedure – when to do it and who has the authority to do it
- Policy on who gets a mobile device
- Acceptable use policy – can the client utilize the device for anything else
- Creation of “in the field” trouble shooting documentation for end users
- Authentication and identification policy and procedures

- Approved software applications - including antivirus and security – what is the base software applications made available on the device
 - Provisioning – procedure on how it is done
 - Standard and base configuration documentation of handheld devices
 - Network Infrastructure – Network Topology how the mobile solutions fits in to the infrastructure and how data, information and processes are handled and secured
- (BlackBerry, 2005) (Ric Liang, 2008)

Conclusion

Blackberrization can be used by most organizations to enhance the customer experience and improve business efficiency. The value of these business related gains needs to be carefully considered before deploying resources towards a mobile platform. Companies must balance strategic deployments against tactical task, task specific projects, so as to maximize the corporate investment and make the best choices in the implementation of platforms and technologies (Gold, 2008). Careful consideration should be given towards management of the handheld mobile device and special consideration needs to be given to the protection of data and intellectual property on the device. Strong commitment from executive management team is required to ensure the success of the Blackberrization project.

Unprecedented growth experienced in the mobility market is here to stay, so letting workers access business data when they want, where they want and how they want will lead to increased productivity, efficiency and sales revenue.

March 2009

Authored by Shanmuga Chittoory, Tuhin Ghosh, Luis Guzman, Edward Jeleniowski, Wing Shan Lau, Shawn Lowery

For additional information on this article, contact Tuhin Ghosh, Software Development Manager at TISCOR, www.TISCOR.com, 858.524.7700.

Appendix A

Symbian is an OS currently found primarily on Nokia Smartphones. It is widely considered to be the first Smartphone designed to successfully targeted by the Cabir worm. Older versions of Symbian were fairly insecure, newer versions (9.x) have better security including individually settable permissions for different applications and rights, but it is still relatively easy for an end user to override permissions set by IT if they wish. Symbian's strength, a large installed user base, is also its weakness security wise as efforts to hack it are more common. (Anonymous, 2008)

Windows Mobile version 6.1 features security support based on software called System Center Mobile Device Manager 2008 (SCMDM). This software allows permissions to be set similar to what can be done with a laptop or desktop remotely, including SMS services. Currently SCMDM 2008 is limited in what it can do, for instance, exceptions cannot be set for a browser to bypass a proxy for local sites. It does have a “wipe and lock” function and can require password security. Since SCMDM is new and untested it is uncertain whether it is truly secure. It has been designed for a single platform so in a mixed Smartphone environment a third party security application might be more cost efficient. (Microsoft Corporation, 2009)

Blackberry uses the Blackberry Enterprise Server (BES) that can set permissions remotely. Blackberry is commonly thought of as the most secure Smartphone platform from a business perspective, with robust security. Despite some concern that Blackberry servers reside in Canada, Blackberry offers DoD approved DES encryption. (Research In Motion, 2009)

iPhone in an enterprise lacks several critical security features. The current generation has no data encryption or remote lock and wipe. Managing iPhone security remotely currently requires the IT department to have the phone in hand or to trust the end user to properly install third party software. (Al Sacco, 2008)

Android is new and currently implementing enterprise level security. This device is challenging as it has little to no exchange sync-ability. New RISC chipsets that will be launched soon will allow Android to produce Smartphones as powerful as some of today's laptops, specifically enhancing processor speed and RAM memory. With these improvements, it may become a very commonly used OS. Likely third party apps will be required to integrate with Android business systems in the near future. (Android n.d.)

Palm has a new OS worth mentioning. WebOS will be released with the Palm Pre, a new Smartphone. This new device will either be Palms swan song or it's rebirth in the Smartphone market, so it bears watching especially for companies that allow users to select their own devices. If this product makes the predicted splash in the market, IT departments may be required to support WebOS. Currently details about using this OS in an enterprise environment are unclear and security information has not been published. (Palm, n.d.)

References

- Al Sacco (2008). Six Essential Apple iPhone Security Tips. *PCWorld* Retrieved February 2, 2009, from http://www.pcworld.com/businesscenter/article/152128/six_essential_apple_iphone_security_tips.html
- Ambige, Gordon (1999). Empowering the decision maker. *Automatic I.D. News Europe*, 13639765, May99, Vol. 8, Issue 4
- Android.com (n.d.). *What is Android?* Retrieved February 24, 2009, from <http://www.android.com/about/>
- Anonymous, (2008). Symbian 9.2 has been hacked! Guide/Tutorial HERE *FinestFones.com*. Retrieved February 2, 2009, from <http://www.finestfones.com/2008/03/symbian-92-has-been-hacked.html>
- Blackberry (2005) Planning to Implement Blackberry. Retrieved February 16, 2009, from http://wp.bitpipe.com/resource/org_990469824_534/Planning_to_Implement_BlackBerry_edp.pdf?site_cd=bpmd
- Cisco (2007, March 9). Improved Patient Care with Mobile technology at the The Children's Hospital at Westmead. *Cisco*. Retrieved February 25, 2009, from http://newsroom.cisco.com/dlls/global/asiapac/news/2007/pr_03-09.html
- Computer Weekly (2005, January 11). Time to mobilize your business. *Computer Weekly*, 1/11/2005, p16-16, 1/4p
- Computer Weekly (2005, April 18). Mobile technology is the fastest growing area of IT expenditure. *Computer Weekly*. Retrieved February 25, 2009, from <http://www.computerweekly.com/Articles/2005/04/18/209474/mobile-technology-is-the-fastest-growing-area-of-it.htm>
- Dragoon, A. (2002). AMF Gets Sales-force Automation Right. *CIO*, 1-5. Retrieved February 2, 2009, from http://www.cio.com/article/31340/AMF_Gets_Sales_force_Automation_Right
- Dedo, Douglas (2004). The return on your mobility investment. *Microsoft*. Retrieved February 14, 2009, from http://download.microsoft.com/download/1/a/5/1a572c42-10b5-469d-9acb-ceed2e634985/MobileDevices_ROI.doc
- Flinders, Karl (2009, January 20). Indian farmers benefiting from mobile technology. *ComputerWeekly*. Retrieved February 25, 2009, from

- <http://www.computerweekly.com/Articles/2009/01/20/234331/indian-farmers-benefiting-from-mobile-technology.htm>
- Gold, Jack (2008, October). *Mobile Applications: A Different Breed*. Retrieved February 12, 2009 from http://research.bizreport.com/detail/RES/1226508895_774.html
- Hospitality.Net (2000, October 3). Carlson Hospitality Worldwide Introduces MACH-1 Wireless, Portable Information Management System. *Hospitalitynet.org*. Retrieved February 24, 2009, from <http://www.hospitalitynet.org/news/4006058.search?query=carlson+mach>
- Johnson, Johna (2007, July 16). Here's why you need a mobility strategy. *Network World*, /16/2007, Vol. 24 Issue 27, p30-30, 1/2p; (AN 25817902)
- Lion, Elsa (2004, July 7). But what is the business case for going mobile? *Computer Weekly* 00104787
- May, Jonathan (2006, April 27). Mobility solutions can save companies millions. *Caribbean Business*; 4/27/2006, Vol. 34 Issue 16, pS4-S4, 1/2p
- Microsoft Corporation, (2009) System Center Mobile Device Manager TechCenter. *Microsoft Technet*. Retrieved February 25, 2009, from <http://technet.microsoft.com/en-us/library/dd252770.aspx>
- Oliver, M. (2008). *Mobile Device Management for Dummies*. West Sussex, England: John Wiley & Sons, Ltd. Retrieved February 24, 2009, from http://www.yucat.com/docs/Sybase_MobileDeviceManagementForDummies_Yucat.pdf
- Palm (n.d.) *Overview of WebOS*. Retrieved February 24, 2009, from http://developer.palm.com/webos_book/book1.html
- Research In Motion (2009). *Wireless Data Security*. Retrieved February 25, 2009, from <http://na.blackberry.com/eng/atagance/security/features.jsp>
- Ric Liang (2008, November 6) *10 steps to a Blackberry Deployment*. Retrieved February 16, 2009, from <http://www.zdnetasia.com/techguide/wireless/0,39044905,61965018,00.htm>
- Sage (2007). *Business on the move*. Retrieved February 15, 2009, from <http://www.sage.co.uk/fitforbusiness/pdf/Sage%201000%20White%20Paper%20-%20Business%20On%20The%20Move%20NB.pdf>
- SharpComm.com (n.d.). *Mobility Improve Productivity while reducing energy consumption*. Retrieved February 24, 2009, from

http://www.sharpcomm.net/mobility_pbx_baltimore_pbx_maryland_dc_virginia.php

SOTI.Net (2009). *Overcoming Mobile Enterprise Security Challenges*. Retrieved February 15, 2009, from <http://www.soti.net/media/securitywhitepapermc.pdf>

Sudan, S., & Drake, S. (2008). Facing the Challenges and the Business Value of Effectively Managing Mobile Devices. *IDC*. Retrieved February 15, 2009, from http://ca.com/files/IndustryAnalystReports/facing_the_challenges_and_the_business_value.pdf

TISCOR (n.d.). *Application Report: University of Connecticut*. Retrieved February 24, 2009, from [http://www.backtrackgroup.com/web/SiteBuilder/TiscorISBv1r0.nsf/Files/University%20of%20Connecticut%20Ap%20Report.pdf/\\$File/University%20of%20Connecticut%20Ap%20Report.pdf](http://www.backtrackgroup.com/web/SiteBuilder/TiscorISBv1r0.nsf/Files/University%20of%20Connecticut%20Ap%20Report.pdf/$File/University%20of%20Connecticut%20Ap%20Report.pdf)

Yankee Group Research, Inc (December 22, 2006). *Enterprise Mobility Is the Last Mile in Sales and Service Effectiveness*. Retrieved February 2, 2009, from <http://www.yankeegroup.com/ResearchDocument.do?id=15057>