Governance of Mobile Technology in Enterprises

Kamal Thakur

Director, GITM
Email: kamal_thakur12@yahoo.co.in

Abstract : Wireless mobile connectivity is gaining ground in enterprises IT strategy and, in many businesses, it is fast becoming critical for survival. Mobile workers often need wireless Devices and applications to access data at office remotely.

Keywords: Wireless technology, Mobile Technology, IT, PDA, Mobile Computing,

I. INTRODUCTION

A research report from Gartner states that laptop computers now comprise nearly a quarter of the PCs used by large enterprises. This mobile computing trend will grow as prices of laptops, smart phones and personal digital assistants (PDA's) continue to drop. Furthermore, such devices come packed with enormous computing power. The latest generation of Pocket PC devices, for example, is rapidly approaching the computing power of laptops, and with the addition of cellular phone and Wi-Fi capabilities.

At price points that are approximately one-third the current price of a laptop, the latest generation of devices frequently has more connectivity options. Currently, many mobile workers are using wireless devices primarily for e-mail. However, it is important to note that the impetus behind mobile computing goes far beyond e-mail. Organizations are also seeking to connect their workforce to business-critical data and processes. Access to back-end system information, enterprises data and process infrastructure is essential to increasing competitiveness, productivity and efficiency. The enterprises gains the advantages of improved response time, faster resolution of customer calls, immediate tracking of warranty information, reduced communication costs and elimination of duplicate data entry, ensuring data accuracy and integrity and balancing of workload across all mobile and stationary workers. All of this translates into cost reduction and increased corporate revenues, along with measurable competitive advantage.

Changes in the PDA market signal a shift from e-mail centric mobile devices to more robust business process automation. The Gartner research report also reveals that market share Microsoft Windows Mobile devices has been growing steadily since 2000 and surpassed palm OS licenses for the first time in the third quarter of 2 004, capturing 48.1 percent of the worldwide market. The rise of Windows Mobile corresponds with a rising demand for open, devices-natural mobile platforms that deliver always-available capability, access to corporate networks and database, easy synchronization between mobile devices and servers, improved data integrity and security, and rapid workflow.

Some of the quick-win mobile deployments with positive return on investments are:

1.1 Sales and field force automation and customer relationship management- Logistics companies now regularly use handheld devices for recording deliveries and instantly updating the data on the remote servers.

1.2 Public utility inspection and even maintenance personnel and census takers

1.3 Public safety and emergencies- Wireless applications are extremely useful in handling emergency situations on the field.

1.4 Travel-Maps and routes are now available on GPS-enabled mobile devices and help speed up travel time.

1.5 "Dead-time" productivity- Mobile data connectivity improve productivity during dead times, such as when people are waiting at airports or for meetings. This time is precious and could be used to check e-mail, respond to urgent requests or fix meetings.

Mobile technology and applications, in many cases, have been successful, and have given a positive return on investments with short payback periods. However, the adoption is still not mature. As per Jeff Moore's Crossing the Chasm Paradigm, organizations are in the second stage, with most early adopters having completed first-round deployments and having begun to evaluate how to proceed with further mobile initiatives, either by extending the mobile solution to a large base (for example, e-mail) or mobilizing other applications.

The technology itself is not mature and is undergoing continuous transformation. Managers have not yet understood the value of mobile and wireless solutions. Moreover, the following hurdles exist and have to be overcome:

- Failure of the ecosystem to work cohesively
- A lack of cooperation, interoperability and standards
- Domination by mobile operators

Most mobile deployments have not been thought through and were implemented without looking for

opportunities to adapt or optimize business process. In most cases, the IT architecture has not been reviewed. Unfortunately, many IT managers see mobile and wireless more as a threat than an opportunity. They fear it may disrupt their security solutions and policies, and bring more work and complexity with additional client platforms to manage. Their fears are not without basis.

Consider this example: A leading commercial marketing firm hired an IT outsourcer to create a 100 percent custom solution for its mobile workforce. From the outset, however, the technology vendor did not appreciate the complexities of mobile computing. The firm spent several months on the project and, in the end; an application was this has created more problems than solutions. The systems became very slow, taking a long time to issue pages of reports on handheld devices. Users who do not want to wait naturally get frustrated with the slow speed, as an end effect the system started loosing data. The data of the project given to the IT outsourcer was not fully synchronized A lot of updated data was not finding their way to mobile Devices. The system also was not equipped with any backend reporting or analysis capability. The entire exercise ended upon chaos and confusion.

Despite failure stories, there are many success stories in the areas identified previously. According to Gartner, by 2008, 80 percent of enterprises would have mobile and wireless deployments to support at least one business process (success rate was 0.7 probabilities). Industry classes that are giants adapt to the changing environment and demand.

Mobile technology in the enterprises include distribution logistics, food and beverage, utilities, construction, non-IT professional services, conglomerates, medicine, and government. Several others are slow to take the line but looking at the benefits there is no way except to come on board. Mobile technology is here to stay and grow. Enterprises should not try to escape its adoption; instead, they need to build a mobile strategy and a governance framework to manage it.

II. DEVELOPING A MOBILE TECHNOLOGY GOVERNANCE FRAMEWORK

The fundamental principal of IT governance have is said to be to manage the increase of Technology risks vis a vis the mobile developments in the field of mobile applicability.

It is necessary that top management commitment is necessary to ensure successful implementation. Ownership by affected process owners is also critical. Strategic direction and proper planning, followed by meticulous execution, are necessary, as with all projects.

Organizations should first develop a business case for mobile deployment. Cost-benefit analysis and risk assessment should be completed at the outset. Technology alone should never drive its adoption, or it is bound to fail. A proper business case needs to be established with measurable success indicators so that a review is possible later.

Many early adopters have set up a mobile center of excellence, which they hope will optimize the use of corporate resources and provide the best chance of success. The center plays an important role in developing standards, publishing information, and planning and performing quality assurance. It also leverages resources from other departments for security and application deployments tools.

As this is a rapidly evolving technology, it is important to plan for obsolescence. The mobile middleware market is consolidating rapidly. Organizations should plan ahead for replacement of tactical product selections. Mergers and acquisitions in the vendor space might require change in tactics. The vendors of development environment and commercial off-the-shelf software are improving their capabilities in this space.

III. ESTABLISH A MOBILE POLICY

A strong policy is essential for governing the use of mobile technology and devices. A good policy should describe proper behavior and stipulate what may and may not be done. The policy should include guidelines on as \-needed usage, coasts and reimbursements, and human resource perspectives, including when people leave the organization.

The support group of some organizations also supports handheld devices, such as PDA's and phones. The groups recognize that these devices are simply different forms of client access devices for which the policies should be similar.

Pc groups provide three levels support:

3.1 A fully supported standard devices, which receives the support privileges of PCs, including application and development support

3.2 Data interface support. This is a device that can be connected to enterprise information sources to retrieve information through controlled ports. Without this application or development support is provided

3.3 Unsupported device, which appears in low volume or that is so custamercentric.

IV. ESTABLISH A SECURITY POLICY AND FRAMEWORK

The risk of unauthorized intrusion into wireless networks does exist. This is quite easy to do when networks are not secure. If the mobile devices risk is

stolen it could cause the repercussions huge. Enterprises data are sensitive and can fall into the wrong hands. There could be bad legal complications if the devise is lost simultaneously causing loss of sensitive data making it vulnerable.

All these look for a comprehensive security policy. The policy must either eliminate use or force compliance that addresses the organization's views on mobility, permissible use, sourcing, chargeback, standards for devices and usage along with support and service levels, security, and governance.

Most adopting enterprises have set up secure wireless networks that are difficult to penetrate. As there is an increasing use of PC operating system in them, mobile devices have become susceptible to the same threats, hacks and viruses. Therefore, all the PC security measures are to be put in place for mobile devices also. Many organizations are installing personal firewall and antivirus program on these devices, with a clear policy that

4.1 Almost all have stipulated that mobile devices should be password protected "key-locked" at all times.

4.2 User authentication process is mandatory to avoid unauthorized access to enterprise data.

4.3 Mobile connectivity has to be allowed on an as-needed basis, and network activity is closely monitored. Comprehensive security and activity logs are to be maintained and reviewed periodically.

V. GROUP USER ACCORDING TO NEEDS

Every enterprise has different needs. One policy may not be suitable for all. Users may be classified into traveling managers, home workers, mobile sales force, and emergency mobile support force and so on. Each class has their own need. For example, traveling managers probably need a personal information system, e-mail, internet access, intranet access and access to the corporate business intelligence system. Therefore, the user groups and their associated attributes should be identified. Attributes might include user type, remote access needs, remote access locations, remote access frequency, and estimated number of users, the business units that have this profile and support requirements.

The applications that are needed and their attributes should then be identified. These include,
5.1 Criticality to business,
5.2 The number of users,
5.3 Present and future service level requirements, and business benefits.

Only at this stage the devices and their attributes are selected. Device attributes include the operating system, networking capabilities, critical features, desirable features, device vendor, service provider, existing installation in the organization, planned number of devices and, of course, cost.

Thereafter, the enterprise should select device for different user groups and restrict usage to a few standards types. Training and education of users and support staff help determine effective use of the technology.

VI. MONITORING AND CONTROLLING

It is easier to deployed mobile device that manage and control them. Controlling mobile devices is like firing at a moving target. However, it is importance to create a control process with key result areas and success indicators. These have to be monitored regularly to ensure effective utilization of resources and return on investment.

VII. CONCLUSION

This brings to a clear clarity that user expectations are growing rapidly, and enterprises need eventually have to incorporate wireless and mobile technologies in their IT delivery infrastructure. There are considerable risks associated with mobility, such as the potential to catapult costs. However, a simple yet comprehensive policy only helps in controlling costs and minimizes other risks. It is necessary to plan strategically and operate tactically to counter obsolescence and rising costs. Finally, continuous monitoring of key success factors and adherence to the policy are critical ensure timely course correction.

REFERENCES

[1] Phillip Lin "Achieving a Smoother Network Access Control Implementation" ISSA Journal, October 2006, P.No 16.

[2] Jason Edelstein "The Greatest Impacts to Security of Wireless Technology – An Australian Perspective" Information System Control Journal, Volume 4, 2006.

[3] Mark Segelov "The Greatest Impacts to Security of Wireless Technology – A European Perspective" Information System Control Journal, Volume 4, 2006.

[4] Anil Jogani "Governance of Mobile Technology in Enterprises" Information System Control Journal, Volume 4, 2006.

[5] Christos K. Dimitriadis "Improving Security Management for Mobile Operators" Information System Control Journal, Volume 4, 2006.