

Distraction and Diversion

Contacts:

Rob Bamforth
Quocirca Ltd
Tel +44 7802 175796
rob.bamforth@quocirca.com

Bob Tarzey
Quocirca Ltd
Tel +44 1753 855794
bob.tarzey@quocirca.com

Stef Coetzee
NetMotion Wireless
Tel +44 7782 167000
stef@netmotionwireless.eu

Peter George
NetMotion Wireless
Tel +44 7860 484787
peter@netmotionwireless.eu

Avoiding user aggravations is key to mobile productivity

Low cost hardware and a plethora of options for connectivity should make it easier for employees to be more productive and take IT access to their point of need. However, outside the perimeter of the business location, additional controls need to be applied to ensure the security and integrity of data on the mobile device and network access. Balancing the need for control with the flexibility given to the user requires care and attention to both mobile strategy and implementation. Mobile users have many challenges facing them as they try to work outside of a managed and familiar working environment. Too many constraints and challenges can distract and divert users from the task in hand, meaning that productivity gains hoped for by deployment of the technology will be lost. This paper looks at how to get the best out of mobile productivity and how to avoid the six most common mobility pitfalls during the planning and execution of mobile implementations.

- **Security**
The key mobility management challenge. It must be tight enough to protect the business assets without constraining or deflecting user productivity. Complex or difficult to use security solutions will at best stifle productivity and at worst encourage users to bypass them. User attitude and acceptance of responsibility is vital to mobile security - it is literally in their hands.
- **Hardware Limitations**
System frailties are tiresome at the best of times, but without the opportunity for immediate redress they can become a real drain on user productivity. Hardware that is too complex and fiddly, easily breaks or is not well suited to the demands of the mobile worker will hinder productivity and impact the success of the overall deployment.
- **Applications**
Businesses are relying on an increasing number of applications and mobile users need the broad application access and performance as much as deskbound employees. Managing the variety of software versions and patch levels on mobile devices can prove troublesome. Furthermore, mobile applications will also need to be deployed and supported on a diverse range of mobile devices, and are frequently subject to intermittent connectivity via wireless networks.
- **Connection Reliability**
The wireless use of applications cannot rely on uninterrupted connectivity. Mobile networks have inherently patchy or intermittent coverage and there are a multitude of connectivity options and networks available. Roaming from one cellular link to another is rarely problematic, but far greater issues arise when moving from one network type to another, say cellular to Wi-Fi as each has very different connection methods.
- **Network optimisation**
In addition to gaps in coverage, wireless networks have less capacity than wired networks. Many applications rely on plentiful and constantly available bandwidth, yet not only do mobile users rarely have this luxury, they are also likely to be working in awkward conditions or under time pressures.
- **Management**
Mobile devices, their contents and their users are more difficult to manage outside the organisation's boundaries,. Larger deployments have a greater potential for diversity of device, connection and user requirements, and therefore present far greater management complexity. In an effort to keep control, too many constraints are often applied, hindering user productivity.

Conclusions

The business benefits associated with mobility are clear, but avoiding a few of the most common mobile implementation pitfalls can help to maximize the productivity of a mobile workforce. A successful implementation has to recognise the pressures and challenges specifically faced by mobile users and look beyond simply selecting devices and applications.

REPORT NOTE:

This report has been written independently by Quocirca Ltd to address certain issues found in today's organisations. The report draws on Quocirca's extensive knowledge of the technology and business arenas, and provides advice on the approach that organisations should take to create a more effective and efficient environment for future growth.

During the preparation of this report, Quocirca has spoken to a number of suppliers and customers involved in the areas covered. We are grateful for their time and insights.

CONTENTS

1. INTRODUCTION.....	3
2. MOBILE, REMOTE OR FLEXIBLE?.....	4
3. THE PRODUCTIVITY PANACEA.....	5
4. PITFALLS TO ADDRESS.....	7
SECURITY.....	8
HARDWARE LIMITATIONS.....	9
APPLICATION PERFORMANCE.....	9
CONNECTION RELIABILITY.....	9
NETWORK OPTIMISATION.....	10
MANAGEMENT.....	10
5. CONCLUSION.....	11
APPENDIX – HOW TO TACKLE THE MOBILE PRODUCTIVITY PITFALLS.....	12
ABOUT NETMOTION WIRELESS.....	13
ABOUT QUOCIRCA.....	14

1. Introduction

Working whilst outside the office, home or other fixed location is nothing new. Long before wireless and cellular networking became widely used for mobile access to IT or communications, service and field engineers, trades people, sales people, and other professionals have often had to perform their job responsibilities outside the confines of their office or business premises and while on the move. For many organisations it is a major benefit to have access to central IT systems at the employees' point of activity, however remote that might be, with information updated immediately, in real time, when and where the transaction is being performed.

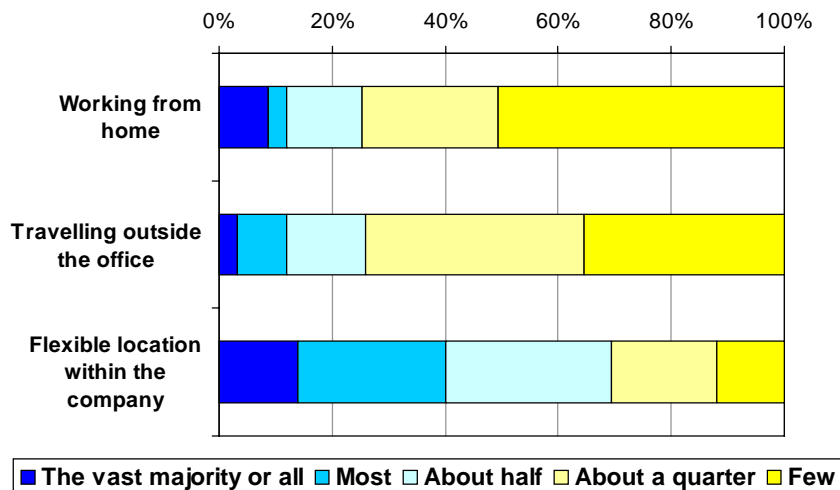
This mode of work is essential to the successful operation of many organisations, and although escaping the constraints of the office might seem liberating to some, mobile and remote working can often be excessively tiring, stressful and highly disruptive. It is also not necessarily the most productive environment for work either, as there are many disruptions and interruptions that can distract and affect efficiency. These are different from those inside business premises – colleagues, other phones ringing, the lure of a coffee machine or staff facilities – and for many employees a mobile workplace will provide a quieter haven from the buzz of an office, but with other temptations and challenges to slow the working process.

The challenge now is that with so many more workers relying on almost continuous access to IT services to perform their job functions, there is an increasing need for mobile or remote access solutions (Figure 1). When the research was conducted, the majority of companies thought that the number of employees in these types of working roles would grow, and anecdotally that trend appears to be accurate. Changes in attitudes to the environment, business facilities locations and working practices provides more impetus for all forms of flexible, mobile and remote working to increase and this will place increasing demands on the IT function. Away from the office, mobile and remote employees cannot depend on the presence or immediate support of colleagues and rely on a communications lifeline to the IT department.

To help them remain at their most productive, these employees must focus as little time, effort and energy as possible on the technology and tools they are provided with, to concentrate on the task in hand. It is bad enough for distractions to be part of the environment for mobile workers, but it is even more of an aggravation when the mobile technology itself gets in the way of productive working.

Figure 1

Working other than at a fixed desk – what proportion of employees would benefit from access to IT?



“Transforming the workplace” – Winter 2005

As this mode of working becomes the norm for many more workers, distractions caused by technology shortcomings should be minimised, otherwise the productivity gains promised by mobile working will be diminished. This document looks at the main areas where problems generally occur in mobile deployments, and how organisations can avoid the pitfalls and therefore maximise mobile productivity.

2. Mobile, Remote or Flexible?

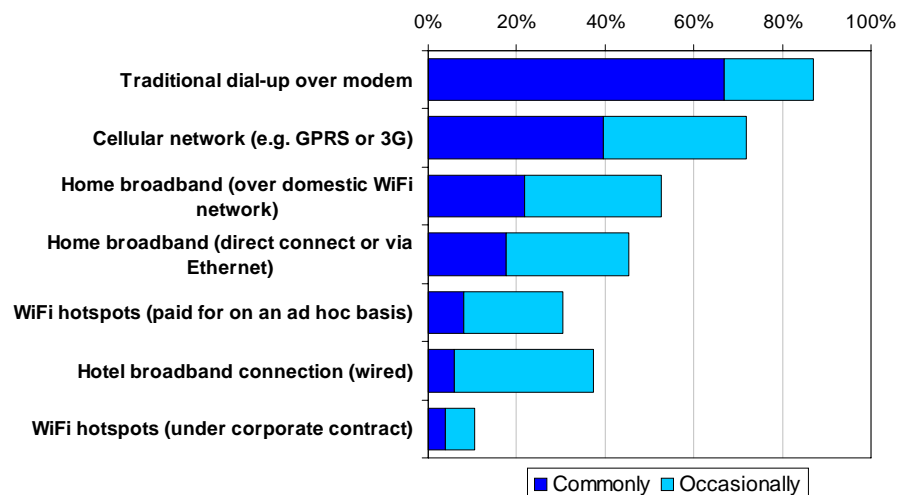
Once the constraints of a fixed desk are removed there are a number of different ‘un-tethered’ ways of working. For example some organisations have some form of flexible working or hot-desking where employees roam among different desks or workstations within the organisation’s facilities. In others, many employees have worked remotely in some form, perhaps from home, or historically by dialling in with a modem over a phone line while travelling, say in a hotel (Figure 2).

An often quoted stereotype for un-tethered working is the “road warrior” who is often referred to as mobile, but primarily moves from one fixed location to another. These remote workers require intermittent IT access and applications use, from one or more fixed locations – home, hotel or airport lounge. This remote access helps extend the working day, especially when travelling, or manage their work/life balance, but rarely involves the need for continuous IT and application access while on the move.

The more recent growth of networked Personal Digital Assistants (PDAs), smartphones and especially laptops with cellular data cards and embedded wireless connectivity is fuelling the trend towards truly mobile working.

Figure 2

How common is it for laptop users to connect remotely over the following?



Wireless data research – Winter 2005

These truly mobile workers, move from place to place as a fundamental part of their normal workday. In the past they may have used specialised devices deployed over a private radio network, and although some may still do so today, the economics of using public networks and commercially available laptops and handheld devices are more compelling. Overall, though, this means these mobile users have a different experience to remote workers and a different set of needs:

- **Near constant connection** – network link should be kept open, inactive if necessary, rather than ‘broken’ then ‘re-established’.
- **High performance expectations** – connection must offer sufficient bandwidth even over wireless networks
- **Office-like support** – applications should ‘just work’ regardless of device type, just like in a desktop or fixed environment
- **Connection diversity** – use a variety of networks to minimise any coverage black spot issues
- **Mobile application access** – all applications must perform competently on a variety of mobile devices and networks
- **Be secure in insecure environments** – over any network, based on corporate policy, but without hindering usability

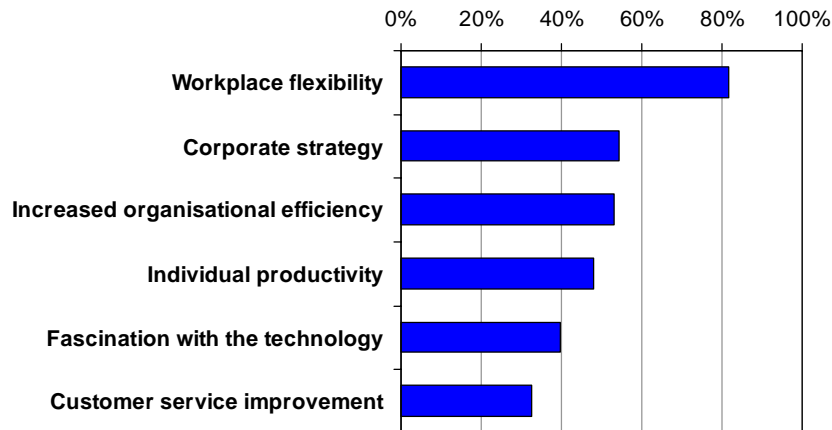
These requirements mean that a different approach must be taken to deploy, manage and secure truly mobile workers and the IT resources they use, otherwise the technology becomes part of the problem rather than part of the solution.

3. The Productivity Panacea

Workforce productivity, the employers' return on the investment of wages and benefits, is often mentioned when trying to compare one country's industrial capabilities against another's. No wonder then that productivity improvements are the yardsticks so often chosen by vendors seeking to sell new products and solutions. But there is an increasing need for businesses to be able to more rapidly adapt to changing circumstances, new competitors, and fluctuations in material and resource costs. Flexibility, organisational efficiency as well as individual effectiveness all play a part in the business productivity for mobile deployment (Figure 3).

Figure 3

What drives the interest in mobile technologies for those with widespread deployment?



"Mobile Security and Responsibility" – Spring 2006

Measuring the value of any investment at any given point in time is often difficult. Knowing precisely what to measure is even harder. In theory it is a simple equation for any business – return over cost – but not all costs or the returns are easy to identify or quantify. Mobile worker productivity is often difficult to measure as there are many softer and less tangible factors that have an impact on the individual's effectiveness and the value of their efforts:

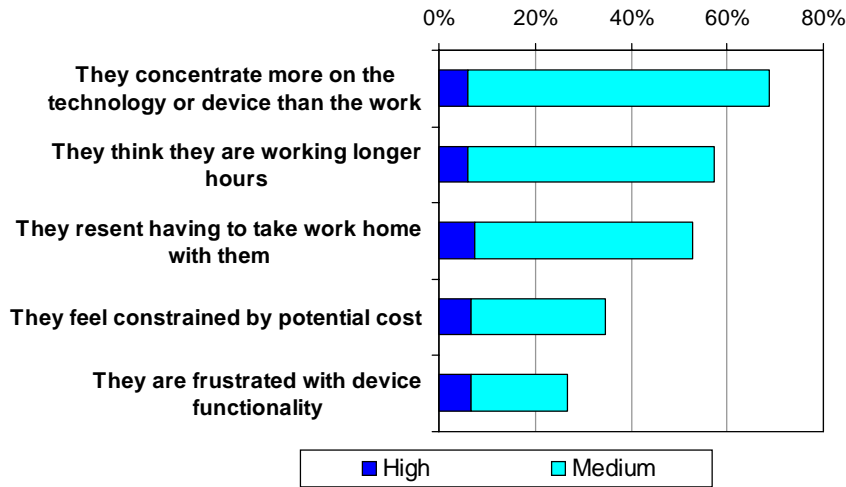
- **Reduced travel** – saving time for organisation and individual
- **Individual control** – subject to workflow needs, choosing the time and place where most appropriate
- **Being trusted** – both with expensive technology and often sensitive information, without constant management scrutiny
- **Work/life balance** – blurred working day boundaries and 'time-slicing' personal and work commitments during the day
- **Self sufficient** – being able to make decisions based on accurate, immediately accessible information

All of these less tangible factors are greatly influenced by the worker's attitude and willingness or commitment to doing the task. For some this will come easily, as their reward follows directly. For example, sales people will look favourably on anything that might help them close their deals more quickly. For others, where work is a chore, anything that appears to make their job more difficult or complex will often be resisted or mis-used. Even where mobile workers follow set patterns or processes that can be measured, such as a field service engineer with a daily list of problem sites to visit, the attitude of the individual is crucial to getting the best results from using technology to speed the process.

As well as the influence of the technology, the change in working practices for mobile employees means there are also management issues to consider (Figure 4). Away from supervision there may be some concerns by managers that employees will not get on with the tasks in hand, and may focus too much effort on dealing with, or playing with, the technology. Some of this is easy to deal with. Mobile devices can be configured in a 'lock down' mode so that additional software can not be added and settings can not be changed by the user. Simple distractions such as games can be removed. However the more likely distractions are from how much the user has to engage with, and fiddle with, the device, applications and connectivity in order to make them work effectively.

Figure 4

How important are these negative impacts on productivity for employees?



“Productivity or Pain” – Winter 2005

The vast majority of employees know they have a job to get on with, and want to make progress. In fact many will work harder and longer because they have the tools to allow them to do so. The danger then is they may resent the extension into what is seen as their personal life. Mobile devices like laptops, mobile business phones and the notorious mobile email, PDA or smartphone devices are not only carried home, they are often switched on well outside regular working hours. Some, perhaps many, will even take them on holiday.

However this is less of a technology issue, and more one of management. It is important in the deployment of mobile technology to temper the overzealous desire to measure everything too tightly, as this will only increase any feeling of resentment. It is far better to measure what is important – the end result – and empower the employee with the tools and flexibility to get the job done. This increases the intangible influences on effective working and providing the technology does not get in the way and make mobile life harder, will increase productivity.

4. Pitfalls to Address

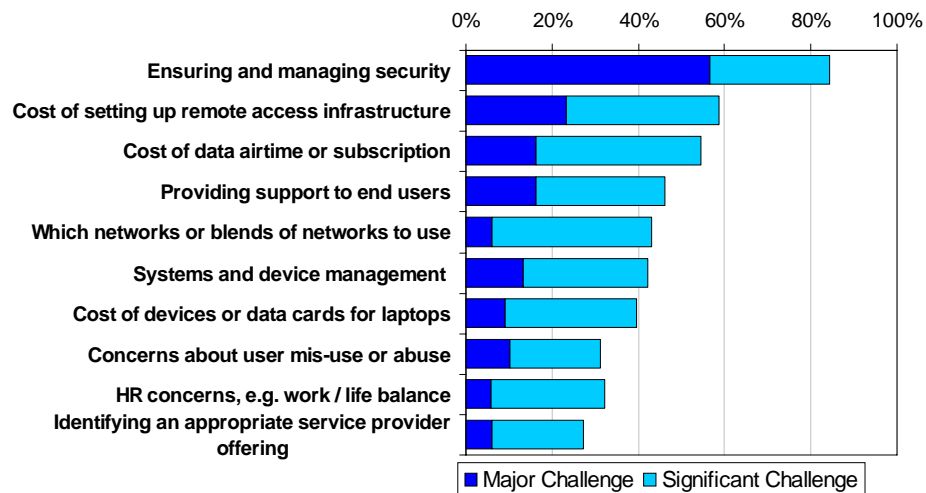
There are many challenges facing any mobile deployment, but security is always the number one issue (Figure 4). This is unsurprising, as there have been many horror stories in the media. Occasionally this might seem like scare-mongering, but the reality is there are many things that can go awry. Devices can be lost or stolen and the data on them and any access granted to them might become available to a third party, and sensitive data traffic can be intercepted when passing over public wireless networks.

Beyond security the next major concerns are centred on the mobile network itself, in particular the costs. While there might be a significant up front investment required to set up the infrastructure, buy devices, software and so on, it is the ongoing costs (Total cost of ownership or TCO) that will have greatest impact. While data costs are variable and based on the amount of actual data transmitted, organisations should minimise any need for users to re-try or re-send data, and wherever possible use some form of compression and transmission optimisation to improve performance. All together these have a direct impact on the greatest cost component, employee time and effort.

The other scale for cost is based on the number of employees who will be provided with mobile access. This has sometimes been seen as a perk for senior managers or those whose requests are loudest. A better approach is to see where the greatest corporate benefit lies. This is where return on investment has to take into account total lifecycle costs, such as support, training and replacement for lost or damaged devices. While some employees may gain good value out of their use of mobile devices, for others those lifetime costs beyond the data airtime or subscription may make deployment prohibitive.

Figure 5

How much of a challenge are the following when considering broad deployment of wireless connectivity to mobile users?



“Commodity or Value Add” – Summer 2006

The process of working out who should be offered what forms of mobile connectivity should be based on a business strategy for mobility rather than on an ad hoc basis. Aspects other than technology, such as the impact on workplace resources, personnel or perhaps employee representative bodies such as trades unions, and staff management issues need to be taken into account to appropriately shape the business strategy for mobile deployment.

This then drives the implementation plan. Most organisations will need to test various aspects of the deployment, and this may mean piloting various devices, connectivity options and solutions with a number of employees. This is a worthwhile approach providing as much information as possible is gleaned about how the technology improves, or perhaps hinders, the working process. It is the best opportunity to identify how mobile employees work with the technology and how well it fits their needs.

To prepare for a pilot deployment, a number of technical decisions have to be made, and solutions chosen. In every category of products there are a number of solutions, but it is worth bearing in mind how choices made at this stage will have an impact on the level of productivity achieved by mobile users. The following mobile productivity pitfalls need to be considered:

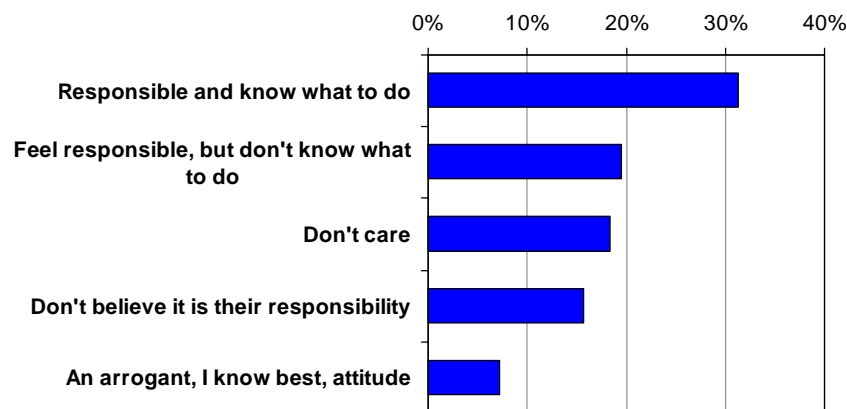
Security

Managing security plays a large part in any mobile deployment. The organisation has to protect the devices themselves, the access they permit back into the corporate network and any data stored on the device or in transit. This can be quite involved and require complex tools, but these have to be selected and appraised against a backdrop of a mobile security policy, based on the business needs. There is no point making some inconsequential information securely protected if this greatly inhibits those using the information as part of their working day.

The choice of security tools and their implementation can have a profound effect on the mobile user’s productivity, and so great care must be taken to ensure that the most appropriate levels of protection are being applied, and that security procedures do not have a negative impact on the user. It is important to realise there are many different mindsets among mobile users and their attitude towards security. While most are responsible and want to do the right thing, a significant number will not be so careful (Figure 6).

Figure 6

What best characterises the attitude of mobile users in your organisation to security?



“Mobile Security and Responsibility” – Spring 2006

When mobile devices are connected to open or public networks, effective levels of security should always be applied. This is especially true for authenticating the user, and preferably the user and device together, and for strong encryption to be applied to the data in transit, using a Virtual Private Network (VPN). A variety of VPN solutions for secure remote access have been available for some time, emerging from those designed for linking sites with point to point protection and those for individuals in remote locations with the growing use of public networks like the Internet. The increasing use of mobile connectivity has now led to a new category of VPN solutions, Mobile VPNs, designed to meet the more challenging needs of securing mobile users.

These Mobile VPN security solutions are specifically designed to meet both mobile use and remote or fixed access requirements, unlike traditional Secure Sockets Layer (SSL) or IPSec VPN solutions which are geared primarily towards remote, fixed access. The application of SSL VPNs emerged with the growth of the Internet and the use of the web browser. This has an advantage in that no specialised client software is required for deployment, and the user can use any device with a browser connected to the network. However this in itself could be a security risk as unknown and unmanaged devices can have malicious software installed on them. A Mobile VPN requires client software to be installed and managed on each mobile device, but allows the communications link to be more fully controlled and secured. With Mobile VPNs, more efficient low level network protocols can be used, allowing optimisation on even low bandwidth links and enabling application sessions to be preserved when connection fails or a user roams across networks. Other remote access or VPN solutions work well for general remote access, but Mobile VPNs should address the complex needs of mobile users as well as remote users.

Security tools should provide a centralised management system to support security policy and enable action to be taken if there is a breach, so that for example in the event of loss or theft, the device can be quarantined. There is also a need to make sure the user understands and buys in to their responsibility to look after the corporate assets in their care. It is very easy to set aside, mislay or forget a mobile device, even a laptop and risk the loss of both data and device. Mobile devices are also seen as desirable or valuable and are vulnerable to theft. It is more effective to give the user some choice over the device they are allocated so they will accept it as a personal, and perhaps personalised, possession entrusted to their care rather than something they are forced to carry.

It may be necessary protect data and applications stored on the device with encryption, but care needs to be taken to ensure this is only applied where necessary as it could become very inconvenient for a user in a hurry. Similarly a simple password login at the beginning of the day might be a slight annoyance, but being asked for the same password every hour is sure to lead to user frustration and distraction. In this case a user will look to find ways around the issue, become distracted and less inclined to work at full stretch, and possibly treat the device with less care. Security measures need to be defined and enforced, but they must fit with the working patterns and needs of the user, not divert them into new patterns as that will hinder productivity. Security steps to be completed by the user of a mobile device should certainly be no more onerous than the IT experience at their desk.

Hardware Limitations

While most IT managers would probably prefer to deploy only one type and configuration of mobile device, some element of user choice and device diversity is inevitable. Some categories of users will be more productive with a specific device type or form of interface. It is hard to see any role that requires the user to wear gloves for example to work well with stylus or touch screen driven interfaces. Similarly there are environments where keyboards, and unsealed connector ports are not conducive to straightforward working. A heavier system with a longer battery life will allow one type of worker to be more productive if they leave the device on all day and 'snack' at usage, whereas another worker might be more happy and effective with a lightweight device, where the potentially shorter battery life is not an issue for their working pattern.

Some choice might also help users feel more responsible for their mobile device as it becomes a tool more personalised to their needs rather than a piece of standard equipment they are compelled to carry because "that's what everyone has". However all choices need to be sanctioned, purchased, configured, deployed and managed, so the pragmatic approach would be to have a limited selection of approved, standard devices. This allows for maximum control and security, while providing some variation to accommodate working patterns and user needs.

Some aspects of hardware will always impact user productivity, and these need to be addressed in the selection and piloting of specific choices. Screens that provide inadequate definition or brightness, flimsy input mechanisms, rapidly shortening battery life are all going to put users off. There are other solutions which look of sufficient quality and appear to perform a useful task – for example biometric security instead of physical or memorised tokens – which do not work when in the hands of the mobile user. When in doubt, pilot and test.

Application Performance

The number of applications used by mobile users can vary significantly. Those in more process-oriented roles may only need one or perhaps two specific applications, whereas others may require the same set of applications that would be available to office users. That might be a regularly used set of four or five applications, but then any number of additional applications might be required only periodically, for example to prepare monthly expenses, company car mileage reports, etc.

At both ends of the scale, application compatibility and performance will be very noticeable to the mobile user and have a dramatic impact on their productivity. Some applications are not written to cope with the challenges of a wireless connection – performance and stability – as they are simply desktop applications being used on the move. Even those that are written specifically with the mobile user in mind are very unlikely to function well in a standalone manner without a reasonable network link and careful integration into the existing backend office systems. In any case, provision has to be made for the intermittent nature of mobile work. A mobile worker may have to suddenly stop, and then restart later when convenient, or some piece of information sought has been found. Rather than the application dictating the pace, this is something that the mobile user will need to do, otherwise performance will suffer.

The whole mobile software stack, from operating system, through connectivity utilities to the applications themselves needs to be managed and periodically updated with patches, fixes and new versions. This process has to be done in an assured manner so that each user has the correct version, but it can not be assumed that all mobile devices can be updated at the same time. The update cycle should fit in with the mobile user's working day commitments.

Connection Reliability

A large cause for mobile user frustration is not being able to get or remain connected, but disconnection is a common occurrence even in the best wireless environment. For this reason it is vital that the connection and re-connection processes can be accomplished as quickly and easily as possible, with the minimum user intervention. While it might be perfectly acceptable to enter a password when first making a connection, it will quickly become tedious if this had to be done whenever there was a temporary disconnection. Yet unfortunately, many mobile users are given tools that are better suited to remote workers who only need to establish a single connection for a whole working period.

Rather than relying on a single form of connection, many mobile users will have several alternative wireless network technologies. Today a moderately specified laptop will come equipped with Wi-Fi, cellular and Bluetooth wireless connection options, either as add-in cards, or increasingly, built-in. Within that, the cellular interface will generally include a high speed 3G/CDMA/HSDPA capability, provide broader GPRS coverage, but deliver slower data performance. In addition, there will be an Ethernet port, and perhaps a built-in modem.

This presents the mobile user with a number of connectivity options that can create unwanted complexity, each having an impact on available bandwidth, cost, range or coverage, and perhaps security. It is best to minimise the burden on the user when possible by creating standard policies and practices. For example, some solutions provide policy management tools that allow an administrator to automate network selection based on their available bandwidth – without requiring the user to evaluate and select the most efficient network accessible. A further challenge is whether the mobile user can carry on working if the connection switches to another bearer. If this disconnection requires re-login or re-authentication by the software or applications on the mobile device, time is wasted and data can be lost. Neither is really going to be acceptable or productive for the mobile user. These inconveniences can be prevented by deploying solutions that offer application session persistence even when there are breaks in connectivity and inter-network roaming capabilities.

Network Optimisation

Not only are there choices of wireless networks and potential disconnections or gaps in coverage to deal with, but the network performance available will always lag that of wired networks with current technology. For applications that require the smooth and prompt transmission of data – voice over IP for example – wireless networks are more susceptible to latency and jitter. Some service providers and carriers may have an inefficient internal network, introducing more network hops than are expected or acceptable to some applications, causing them to fail, or work sporadically.

These attributes of mobile networks should not have to be handled within the applications, which will most probably have been architected for a connection-oriented environment. This would be inefficient and impractical. The mobile user experience can be improved, however, with flow and data management tools providing caching, intelligent re-ordering of protocol requests and compression. Some remote access technologies integrate policies for ‘traffic shaping’ to improve performance on bandwidth-constrained networks. The level of value returned in terms of network optimisation will be application or data dependant, but will be most noticeable and appreciated by users of the slower network links.

One potential downside, especially with compression, is the relationship between optimisation and security. The optimisation occurs at the lower levels of the network stack with security processes, such as the encryption of a VPN layered above. Where these are provided by separate solutions, the benefits of compression can be lost as the data is encrypted before compression, and most encrypted data streams lack the patterns apparent in the plain data, which is often where compression algorithms provide the most benefit. To get the most from both optimisation and security, look for a solution that includes both.

Management

The management procedures set the tone for how effective a mobile deployment will be. The personal side of management dictates how comfortable both the mobile worker and their manager will be with business processes conducted outside the company premises. From the employer’s viewpoint, will the employee’s performance be measurable, will he/she be productive, and overall can they be trusted? From the employee’s perspective, how onerous will their commitment to using a mobile device be, what is expected of them, and are there clear guidelines to support them with mobile policies and procedures?

The approach taken to the IT management of mobile users has to take into account the needs of the business, especially from a security perspective, the needs of the users from a flexibility and ease of use perspective, and the ability and resources of the IT department to deliver. This means a centrally managed approach, where configurations and policies can be defined centrally and then applied globally to all suitable devices, but also specifically based on the individual user. Only with a solution providing this level of policy management, can an IT department hope to have sufficient flexibility to have the right level of control at both the device and user level, and be able to scale to larger or more complex deployments as the needs arises.

5. Conclusion

Expecting any deployment of new technologies to automatically provide immediate productivity gains is naïve and demonstrates a tendency to fall for the unsubstantiated marketing claims of vendors. To get the best out of any technology its deployment must fit with business needs and support those whose roles drive the key business processes. Make them more effective and the business is more productive and more profitable. Then, test product and service vendor marketing claims through field trials and evaluations.

Those who chose, are asked, or need for their job role to be mobile will undoubtedly now require access to IT services while on the move. This is an opportunity to affect the business processes for these employees by providing them with suitable mobile tools and devices. But if this is implemented badly, the technology will be too burdensome or complex, distracting the user and lead to frustration or inefficiencies. Organisations will then miss out on the anticipated productivity gains.

By taking a strategic business view of the value and need for mobile working and combining it with a solid understanding of the day to day needs of mobile employees, businesses can get closer to maximising the real benefits of mobility. This is not only the direct tangible impact on mobile employee productivity, but also an increase in flexibility and responsiveness for the business, and an increase in flexibility, control and hopefully satisfaction, for the employee.

APPENDIX – How to tackle the mobile productivity pitfalls

Plan ahead - All too often the hastily implemented ideas of one or two enthusiastic individuals evolve into company policy. There are many ways that mobile technologies can be used, and many technologies to choose from, but the direction should be commercially driven and focus on business needs. Start with a business strategy for mobile deployment, and use this to define the framework in which technical and implementation decisions are framed.

Test - Mobile technology is becoming more robust and widely used, and while it might not be necessary to prove the concept, it is often very worthwhile to test specific attributes for a larger implementation. All businesses have slightly different needs, workforces and working processes. Before moving to a widespread deployment, pilot the solutions selected, and see how they work in practice with real mobile workers performing their regular tasks.

Generate user buy-in - Involve end users right from the outset in the selection and piloting processes. While many employees do not care which IT hardware and services they are offered as long as they work, mobile access is more personal. Mobile devices, from laptops to the mobile phone, make a style statement about the individual. When applications are being used in mobile locations, outside a controlled office environment, user understanding and acceptance of the tools they have been provided with rises in importance.

Mobile security policy - Again, this has to be based on the business needs, fit with any over-arching security policy and balance out the mobile risks against the potential reward. Too tight a security policy will undermine the flexibility and value that mobile working brings, so a pragmatic approach is required. A policy does not have to be a heavy weight document, just something that sets out the organisation's views, objectives and approach to security. Make sure it is well communicated and understood. Support and enforce it with suitable procedures and tools.

Support not strangle - Mobile users and devices must be managed to ensure the corporate assets are kept safe and secure, but this should not hamper the users' ability to work naturally. Better to use systems and processes that make it simple to report faults or problems, and respond quickly to close them down, rather than being overly prescriptive from the outset. Try to keep technology usage as seamless as possible to minimise mobile workers from having to 'context switch' from one train of thought to another.

Align tools to mobile needs – There are a vast range of solutions available, but not all are specifically designed to meet the needs of mobile users. Extending solutions that were designed for remote access will only cause mobile users problems and will lead to frustration, with subsequent impact on productivity. Choose tools that are designed for the more demanding needs of mobile users, rather than trying to make do with those only suited to remote access users.

Anticipate complexity - Mobile users will generally need the greatest range of alternatives for connection. This means dealing with a diversity of network types and choices. The cost and performance of each will vary greatly, but this should not be presented to the user as a consideration during their normal working process. Where possible, make best effort choices based on business policies and the needs of the user. Similarly with devices, expect variant. While it might be preferable for the IT manager to limit the choice of mobile devices to one standard build, this is not going to work for all users, and as technology evolves, it is going to be very hard to maintain for larger and ongoing deployments. This diversity and complexity also must be factored into the management planning.

Stay flexible - For many mobile worker deployments it is still early days. Things can change and deployments may need to scale quickly. New connectivity options may provide high speed networking for some users in the right locations, but may not be evenly spread, or evenly available. Try not to plan too far ahead, or be defensive of tools that work on a small scale, but do not quite meet the larger requirements. Keep a watching brief on suppliers and the rest of the market, with an eye to periodically reviewing selections made.

About NetMotion Wireless

NetMotion Wireless is the industry leader among Mobile VPN solution providers, with over 1,000 customers globally.

Mobility XE™, the company's flagship product, enables hundreds of thousands of mobile workers to get connected and stay connected to critical business applications over wireless networks. Because of its outstanding technology, Mobility XE has received more than 20 product awards, including an Editor's Choice designation from Network Computing.

NetMotion Mobility XE, was recently declared in a survey of over 18,000 customers and prospects as the most trusted VPN to:

- Minimize the security risks of transmitting personal or commercially sensitive data over insecure public wireless networks.
- Eliminate the productivity and data losses which occur when applications crash due to intermittent wireless connectivity.
- Reduce the cost of staff training, and improving the user experience by invisibly handling the complexities involved in managing multiple wireless connections.

To date, Mobility XE is the only Mobile VPN to be certified by Microsoft to run on Laptops, Tablet PCs, Windows Mobile 5.0 PDAs and Smartphones.

For more information about NetMotion Wireless or its products, please visit <http://www.netmotionwireless.eu>

Contact:

NetMotion Wireless
Tel: +44 207 871 0990
Fax: +44 207 691 9487
Email info@netmotionwireless.eu

About Quocirca

Quocirca is a perceptual research and analysis company with world-wide research capabilities and a focus on the European market for information technology and communications (ITC). Its analyst team is made up of real-world practitioners with first hand experience of ITC delivery who continuously research and track the industry in the following key areas:

- Business Process Evolution and Enablement
- Enterprise Applications and Integration
- Communications, Collaboration and Mobility
- Infrastructure and IT Systems Management
- Utility Computing and Delivery of IT as a Service
- IT Delivery Channels and Practices
- IT Investment Activity, Behaviour and Planning

Quocirca research is always pragmatic, business orientated and conducted in the context of the bigger picture. ITC has the ability to transform businesses and the processes that drive them, but often fails to do so. Quocirca's mission is to help its customers improve their success rate.

Quocirca has a pro-active primary research programme, regularly polling users, purchasers and resellers of ITC products and services on the issues of the day. Over time, Quocirca has built a picture of long term investment trends, providing invaluable information for the whole of the ITC community.

Quocirca works with global and local providers of ITC products and services to help them deliver on the promise that ITC holds for business. Quocirca's clients include Oracle, Microsoft, IBM, CA, O2, Symantec and Cisco. Sponsorship of specific studies by such organisations allows much of Quocirca's research to be placed into the public domain. Quocirca's independent culture and the real-world experience of Quocirca's analysts, however, ensures that our research and analysis is always objective, accurate, actionable and challenging.

Many Quocirca reports are freely available and may be downloaded directly from www.quocirca.com.

Contact:

Quocirca Ltd
Mountbatten House
Fairacres
Windsor
Berkshire
SL4 4LE
United Kingdom

Tel +44 1753 754 838
Email info@quocirca.com

The logo for Quocirca, featuring the word "quocirca" in a lowercase, sans-serif font. The letters "quoc" are in blue, "irca" is in black, and the dot over the "i" is in red.