Quocirca Insight Report

June 2005

Mobile Devices and Users

Keep mobile working safe, secure and under control

Contacts:

Rob Bamforth
Quocirca Ltd
Tel +44 1264 393359
rob.bamforth@quocirca.com

Dale Vile
Quocirca Ltd
Tel +44 1425 620008
dale.vile@quocirca.com

Orange Media Centre
Tel +44 207 984 2000

Working with technology outside the office brings many challenges. Use of laptops has grown from limited user communities to widespread desktop replacement and broad deployment. The complexity of managing these devices outside the walls of the office is something IT departments have learned to address. Remote connection has extended from fixed location dial-in to wireless on the move, and smart handheld devices such as PDAs have become networked, converging with mobile phones. This larger and more diverse community of mobile users and their devices increases the demands on the IT function which has to secure the device, data and connection to the network, keeping control of corporate assets, while at the same time supporting mobile user productivity.

KEY FINDINGS

- **Experience reduces overall anxiety, but heightens awareness of specific needs**
  Security fears although still significant, gently decrease with greater experience, and those with broad wireless laptop experience placed less emphasis on this aspect for the deployment of smart handhelds. However experience of smart handheld deployment boosted the numbers seeing the need for increased provision of user support and training.
- **For laptop security, people are the weakest link**
  Anti-virus software, secured VPN access and personal firewalls are deployed by over two thirds of IT professionals, but those with broad wireless experience regard loss, damage or unauthorised use as the major concerns, and these depend on the care taken by users and well communicated security policies.
- **Wireless connectivity does little to increase the burden of managing laptops**
  The cost and complexity of device management is seen as an issue by around half of IT professionals. However the level of challenge perceived to affect security, device management and user support is unaffected by broader experience of wireless laptop deployment.
- **Laptop experience changes the view of starting a smart handheld pilot**
  The key concerns for starting a smart handheld pilot are security and cost of devices, but these lessen for those with broad wireless laptop experience. However the concern over choosing the most appropriate device rises with experience and users cite further concerns over interoperability and compatibility.
- **There is naivety and/or neglect in smart handheld security**
  While plenty of emphasis is placed on security, a worrying number of IT departments do not enforce security for smart handhelds as well as for laptops or they leave it in the hands of users. This is more prevalent in those with limited or unofficial smart handheld activity, but even among those with broad experience, almost a third do not treat smart handheld security as seriously as laptops.
- **Rules rather than technology keeps smart handhelds usage in check**
  Businesses with existing experience of smart handhelds favoured a policy of controlled deployment, with almost two thirds providing a limited choice of devices, and only one third using a technology solution based on continuous synchronisation. However broad experience increases the use of other automated solutions, such as centralised software management and remote device deactivation.

RESEARCH NOTE:
The primary research data upon which this report is based is derived from 2853 online interviews conducted in the second quarter of 2005 on behalf of Orange. Respondents were predominantly IT professionals, representing a mixture of supplier and end user organisations. Geographic location was not specifically identified, but based on primary operator selection, just under half are outside the UK.

CONTENTS

1 Introduction

When information technology was kept locked in machine rooms administered and controlled by a small number of specialists it was easy to manage and keep secure. As it spread through the office to departmental servers and then desktops, bringing everything under control became a major challenge, but at least one that remained within the physical boundaries of the office.

Once systems or access to them leaves the office a new set of problems arise. These are compounded by the shrinking size and increasing diversity of devices which can be lost, forgotten or stolen with relative ease. According to a recent survey interviewing Taxi drivers, thousands of laptops are left on the seats of Taxis in cities around the world everyday. Smaller devices fare even worse, with even greater numbers of PDAs and mobile phones left behind.

This report examines the issues involved in managing and securing this diversity of mobile devices and how businesses can nurture good practices. It is intended to be read by managers with existing mobile projects or those who are embarking on new projects, either initial pilots, or extensions of existing deployments. It offers them a peer review and information for discussion both internally, and with existing or potential suppliers.

As background to the report, online interviews were conducted in connection with a popular online news site, to identify the major challenges, and how they were being dealt with by users and IT managers today. Of the 2853 respondents, 29% had broad experience of wireless laptops, 14% had broad experience of smart handhelds, with around a further 60% in each case having more limited or unofficial experience.

2 Challenges of mobile devices

The term 'mobile device' includes many products in what is a rapidly evolving area, but this report focuses on laptops, and smart handhelds. Laptops include notebooks, tablets or portable PCs based around the Microsoft Windows operating system.

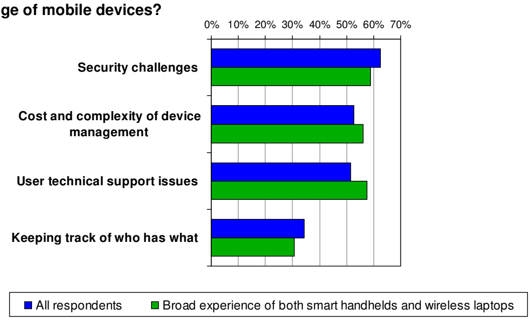
Smart handhelds are defined for the purpose of this report as handheld or pocket-able devices that connect to a wireless or cellular network, and can have software installed on them. This includes networked PDAs and smartphones, and the report uses the term 'handheld' as an all-embracing term.

Mobility brings two main challenges to IT: information is being taken outside of the physically controlled environment on the device, and remote access back to the protected environment is being granted.

The risk has to be balanced with the benefits gained from mobility or remote access. The challenges are widely recognised, but the experience of deploying mobile technology, from laptop remote dial-up through to email pushed to the user's mobile phone, affects the perceptions of importance (Figure 1).

Figure 1

Many organisations deploy a mix of laptops, PDAs, smartphones - which of the following are the most important issues for managing a diverse range of mobile devices?



Security is always a primary concern, but those with some broad experience realise that more often the problems are related to people, rather than just the technology.

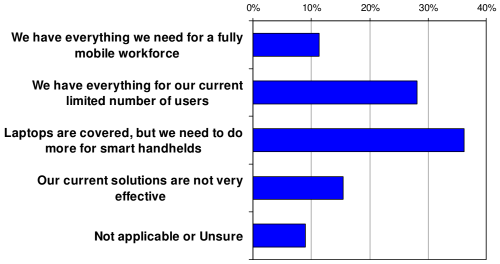
There is still some short-sightedness. Even those with broad experience fail to see the long term significance of keeping track of who has what. Not only do the assets have value, but when an employee leaves, it is important to remove logical as well as physical access to corporate resources.

Devices which belong to the company should be returned to the IT department and at the very least, deactivated and cleansed. Employees should be encouraged to register any devices they provide for themselves with the IT department, so that access can be provisioned in a controlled manner, and de-provisioned appropriately when the employee leaves.

An element of paranoia and understanding of one's own limitations is a good thing, and few believe they have everything in place for full mobility, but overall most think their approach is moderately effective (Figure 2).

Figure 2

How effective are your current solutions in coping with the security, management and user support needs for mobile devices?



There is a reasonable degree of confidence with laptops but the challenges associated with the increasing use of smaller handhelds are clearly recognised.

Unlike laptops, which due to their expense are generally provided as a corporate item requiring significant signoff, many handhelds can squeeze under approval limits, or be purchased by the individual. Their usage often falls outside the range of the IT department's radar.

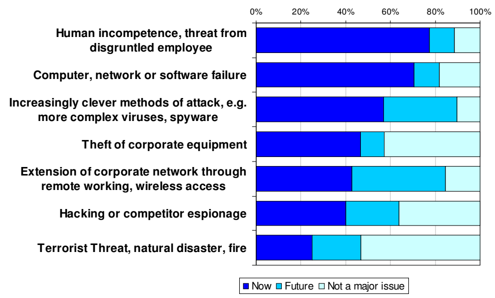
Early handhelds were expensive and specialised, so were deployed only for specific applications, but more general purpose models are now available at relatively low cost, often bundled with a tariff for wireless connection.

These are no longer just the must-have, latest gadgets for the technology aware, but are often valuable productivity tools for business users and occasionally justified by those trying to create an impression of belonging to an overworked elite.

When Quocirca explored general corporate data risks last year[1], remote or wireless access was not seen as the highest current threat, but the one growing most significantly in the future (Figure 3).

Figure 3

What do you feel are the major causes of corporate data risk, now and in the future?



From 'IT Security – Bridging the Gap' – Summer 2004

However many of the other identified causes of risk are increased by the use of mobile access. Smaller devices outside the physical protection of the office are more vulnerable to theft, loss or damage. They are also susceptible to unauthorised access and malicious software such as viruses.

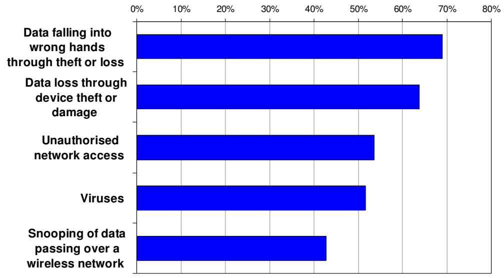
When passwords are compromised or access points breached, the cost to fix and restore is compounded by a loss of credibility. Private data inadvertently made public may cause a crisis of confidence. This tends to have a greater impact on the business than the individual employee, but is often caused by someone's lax behaviour or carelessness.

No one knows what lies around the corner for mobile devices as those with mal-intent seek to exploit their vulnerabilities. So far the often mooted mobile virus has yet to become a major problem, but when it does, the management issues will be more complex.

The first step is to recognise the scale of the challenge, and where to apply the most effort. Despite much adverse publicity concerning the problems of computer viruses, both real with laptop computers, and still relatively theoretical with handhelds, those with broad experience of both are more concerned with losing data (Figure 4).

Figure 4

What are the most important mobile security issues? (Those with broad experience of both wireless laptops and smart handhelds)



It is important for device management to include educating users to take some personal responsibility for the physical security of their devices, as many IT managers have learned from bitter experience.

3 Coping with laptop users

Many of these issues have been recognised with increasing laptop usage over a number of years. The problem now is magnified as laptops are more widely deployed, both to an increasing number of mobile employees, but also as desktop replacements and as a means to take work home.

Larger numbers not only increase the scale of the challenge, but also its scope as a wider range of user skills, knowledge, and diverse round the clock connectivity needs add further complexity.

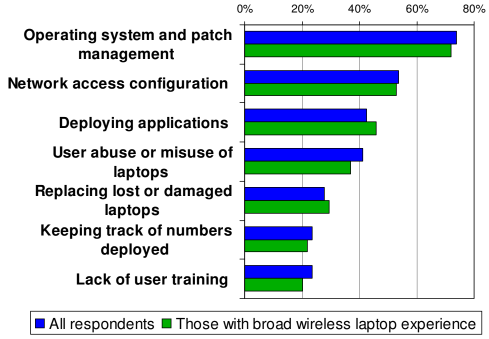
Many of these issues apply to handhelds as well as laptops, but the next sections will use current experience with laptops to highlight the challenges, before moving on to see how these issues apply specifically to handhelds in section 4.

3.1 Managing the laptop itself

The software assets on laptops become more complex as more applications are used on an increasingly sophisticated operating system with diverse connectivity options. Operating system and patch management is seen as the biggest laptop support issue followed closely by network configuration and applications deployment (Figure 5).

Figure 5

What are the most important management or support issues for laptops?



Those with broad experience of wireless laptop usage have similar views to those without. Wireless connection does little to make the device management situation worse, or better. The truth is, most of the challenges are independent of network connectivity. The policies and procedures put in place for laptop support have evolved over the years to be able to cope successfully with managing laptops, connected by wireless means or otherwise.

3.2 Dealing with the user

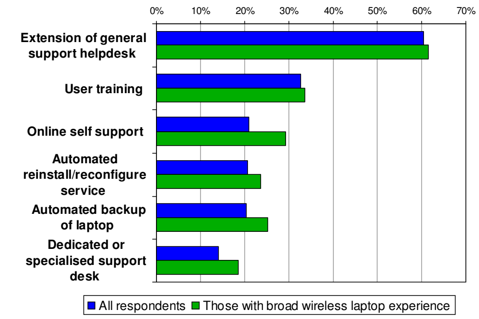
The user oriented aspects of laptop management in Figure 5 appear less problematic than those associated with the laptop itself, with less than a quarter noting lack of user training as an issue. However a worryingly significant number are concerned with user abuse or misuse.

This is most likely to be simply lack of care or neglect rather than deliberate damage, but it is another area where user training could play a positive role, especially if coupled with a strong policy on replacement. Lack of care by the user is something that should be addressed, as it has an important impact on security.

Helpdesks are the preferred solutions for user support, with the emphasis on using the general support function, rather than a separate support group for laptops (Figure 6). This is the right approach, provided specialist help can be quickly reached through the regular support channel. Initial helpdesk contact should route calls to the right expert to avoid callers being passed from one engineer to another.

Figure 6

What processes and solutions are in place for laptop user support?



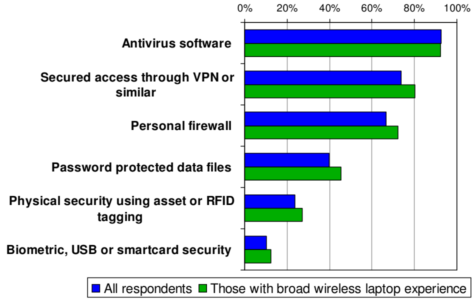
The increased incidence of online self support makes good sense for those with broad wireless laptop usage. Not only are wireless users more likely to be able to make a connection to an online service, they are also more likely to require support outside office hours. This also increases the value of automated backup and reconfiguration, but these are still only used by around a quarter of those with broad wireless usage.

3.3 Dealing with external threats

Awareness of network threats is high for all users and only a little higher for those with broad wireless experience. Scare stories in the media, and availability of increasingly simple to use security tools with automated updates means there is widespread deployment of security software. Most are now getting the message about protecting the software and operating system on the laptop with antivirus or firewall protection, and using it over a secured connection (Figure 7).

Figure 7

Which of the following security solutions do you have in place for laptops?



However if the laptop itself falls into the wrong hands, few deal with the vulnerability of data stored therein. In most cases a thief will be more interested in the value of the laptop rather than its contents, but encryption though tiresome should be considered for data that is very precious or secret.

Fewer still make use of physical means to control access through a biometric reader, smartcard or USB access dongle. These technologies are not new, but they are cumbersome to use, and a solution using secure tokens checked and centrally managed is more practical. Passwords, even if properly used, are rarely sufficient to fully secure access to a portable PC, and the combination of a carried token with a password takes security a step further.

4 Adding the diversity of smart handhelds

Laptops are well understood by users, but handhelds have a different pedigree and are often seen more as consumer electronics than information technology.

Handhelds have had patchy usage in most organisations. Where strong business cases can be made for specific applications which directly support the business process – meter reading, delivery signature recording, field service job handling – there have been some widespread deployments.

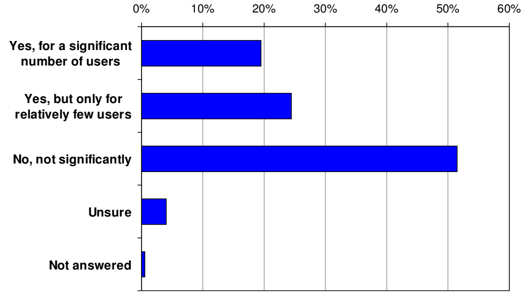
The use of general purpose handhelds, such as PDAs has been more mixed, with widespread backdoor usage by early adopters. This changed with the arrival of the BlackBerry and mobile email. The growing popularity of mobile email combined with the prodigious penetration of the mobile phone is changing the landscape for mobile IT and telecommunications.

4.1 Replacing or augmenting?

Today it is very hard to see a handheld replacing the need for a laptop for existing laptop users. Earlier research[2] shows there is little appetite for any significant replacement of laptops by handhelds in the near future (Figure 8).

Figure 8

Do you see wireless PDAs and smartphones replacing laptops in the foreseeable future?

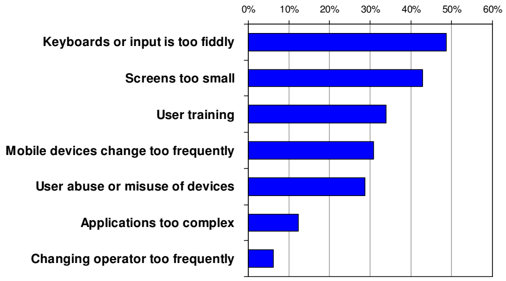


From 'Enterprise Wireless Update – Scaling it up' – Summer 2004

Those users who need to input text, or view intricate documents or figures are unlikely to ever be satisfied with a smart handheld. These limitations are the main challenges to supporting users on handhelds, which are still best suited to less intensive user interaction, quick reference and quick response applications (Figure 9).

Figure 9

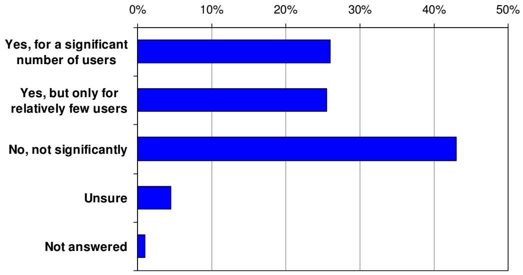
What are the problem areas in supporting users of smart handsets?



Smarter mobile phones are another matter entirely. Not only is the technology evolving rapidly, but the industry encourages the habit of mobile handset upgrades on a far more frequent basis than desktop computers or even laptops. Still, from the same earlier research[2] only a quarter see a significant replacement of voice oriented mobile phones with smart handhelds (Figure 10).

Figure 10

Do you see wireless PDAs and smartphones replacing traditional voice oriented mobile phones in the foreseeable future?



From 'Enterprise Wireless Update – Scaling it up' – Summer 2004

There are many reasons for this. Cost is certainly an issue, but the challenges of security, user support and device management widely known and dealt with for laptops create new uncertainties for the widespread deployment of smaller and more diverse handheld devices.

4.2 Starting a deployment of handhelds

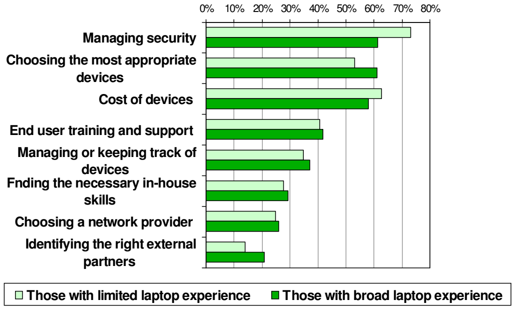
The first issue to deal with is a simple 'why deploy them at all?' Where a business case can be made, suitable technology can provide return on investment, but a clear need or business case is often either not identified, or poorly communicated.

Decisions are often driven by a desire for the latest 'toy' or 'cool gadget' rather than something suited to a business need. Many have had bad experiences with poor quality devices, immature software or short battery life and see the market as too fragmented.

When a business case can be made, the most important issues for starting a handheld pilot are security and cost of the handhelds (Figure 11). Quocirca found in earlier research[3] more interest in wireless or cellular cards for laptops than smart handhelds. The incremental hardware cost is low, and as seen in Figure 5, the addition of wireless does not unduly change the challenges of laptop management.

Figure 11

Which of the following are important issues with regard to starting a pilot with smart handheld wireless devices?



Broad laptop experience softens the concerns surrounding security and hardware costs, but raises the issue of selecting the right handhelds. The large variety of platforms available, with no clear leader makes this a real challenge. Those embarking on pilots should look for guidance from their hardware or software suppliers and network operator, and if possible, trial more than one type of handheld to gain wider experience.

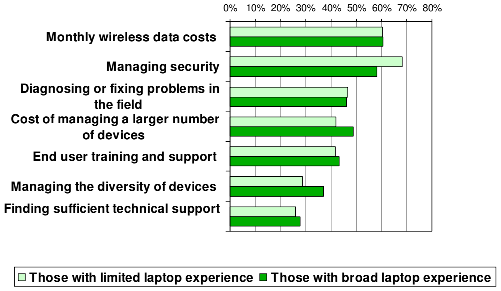
4.3 Scaling up

The reality is that many smart handheld deployments have not yet moved beyond the pilot or proof of concept phase. Even where business cases are fairly clear, pilot projects are a useful way to determine unseen or difficult to quantify benefits.

However the costs and challenges change when scaling up to a large deployment. Levels of knowledge and commitment will vary in different users, so a single type of handheld may not be suitable for all, and the scale of recurring costs, such as airtime, becomes more visible (Figure 12).

Figure 12

Which of the following are important to extending beyond a pilot to a broader deployment of smart handhelds? (Those with broad experience of Smart Handhelds)



Those with broad laptop experience see different challenges in the scaling up of smart handheld deployments, with an increasing awareness of the cost of managing a large number of devices. The differences in operating systems among handhelds, and between smart handhelds and desktop computers means interoperability and compatibility are frequently raised by IT professionals as problems with smart handheld deployment.

The issue of security is still significant, but reduces for those with laptop experience. There are still gaps to fill in the security market for smart handhelds, but the experience of setting and enforcing laptop policies is a good starting point for considering the challenges of smart handhelds.

5 The broader issue of security

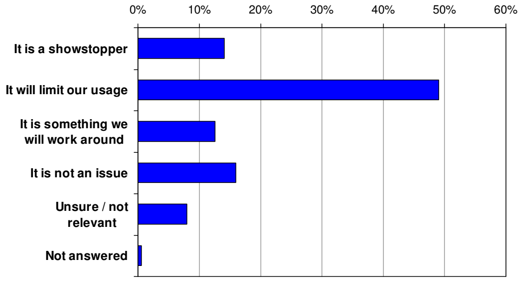
Laptop security is well understood, as issues concerning viruses and firewall protection are common with the desktop PC, especially since Internet connectivity became so prevalent during the 1990s. There are still legitimate fears over the ease with which laptops can be lost or stolen, but overall the approach to laptop security highlights good practices for the deployment of handhelds.

Security can never be absolute, and somehow the cost of losses has to be mitigated. This can be achieved with a suitable insurance policy, but for many the expense may be prohibitive and purchasing replacements as and when necessary, might be a suitable cheaper option. Placing part of the onus or cost on the user in the event of carelessness may also be worthwhile.

Smart handheld security concern diminishes a little with broader wireless experience, but it has been a major factor for some time and few think it is a non issue or something that can be worked around (Figure 13).

Figure 13

How much is the concern over security an inhibitor to rolling out GPRS access for PDA, wireless email device or smartphone users?



From 'Enterprise Wireless Update – Scaling it up' – Summer 2004

The 'fear of the unknown' associated with security issues can be handled with the right support and communication of policies, to ensure that all employees, from the top to the bottom of the organisation are aware of their responsibilities.

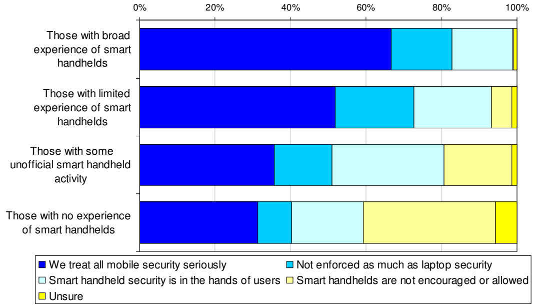
Feedback from IT professionals indicates that more user education of the financial and security ramifications of their actions would be worthwhile. Handhelds are viewed as disposable gadgets rather than precious access points, and those fortunate or senior enough to have them often want to keep upgrading to the latest versions.

The consumer goods appearance and styling is deceptive. It leads to user impatience and an increased incidence of avoiding official routes, bringing handhelds in through the back door, and potentially compromising security.

Attitude has a great deal of impact on the effectiveness of security, and given the concerns raised about smart handhelds, it is surprising that many do not yet take their security sufficiently seriously. Too many of those with even broad experience leave handheld security in the hands of users, or do not enforce it to the level of laptop security (Figure 14).

Figure 14

How does your attitude to mobile security differ for smart handhelds from laptops?



Even in organisations where there is no official usage or support, there must be a policy. It is naïve for business or IT management to ignore the challenge.

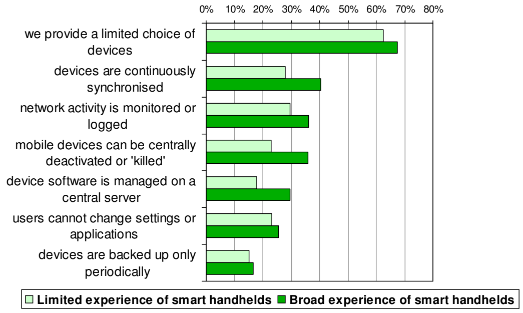
A policy alone is not enough, it must be communicated effectively and enforced so that employees of all levels understand their individual responsibility, and what support is available to them.

6 The user support challenge

The diversity of smart handhelds poses a challenge, but mobile middleware can insulate the differences between most varieties of mobile devices, including laptops. These technology solutions are well established and mature, but the simple alternative of limiting choice is viable too (Figure 15).

Figure 15

What policies and solutions for device management do you have in place for smart handhelds?



While the limited choice approach is the most popular way of dealing with user support for a significant number, the tools available provide additional benefits which are more noted by those with broader experience.

Remote synchronised control from a central server not only ensures the device is configured as expected and therefore reduces the support needs, but also provides a degree of automatic security in the event of user carelessness. Remote deactivation or wiping of data is essential for addressing the major security issues raised in Figure 4 – keeping the data on the handheld from falling into the wrong hands.

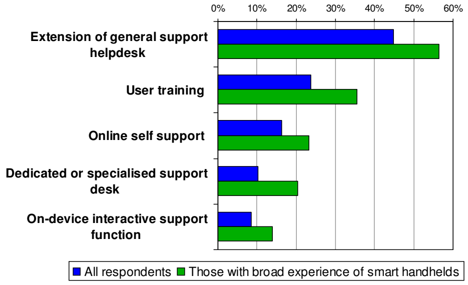
Technology does not fix all problems, and any policy should start and end with good communications to ensure everyone within the organisation knows how to use their handheld devices appropriately and fully understand the consequences of their actions.

Many IT professionals regard users as the weakest link, and the hardest challenge is to establish the right attitude and behaviour among users. Indifference, bad security habits and being oblivious to the real risks lead some to believe that only strong measures will suffice.

There are again lessons to be learned from laptop support and it is not surprising that those with broad handheld deployments put more effort into supporting users, but still relatively few use on-device functions to provide interactive support (Figure 16).

Figure 16

What processes and solutions are in place for smart handheld user support?

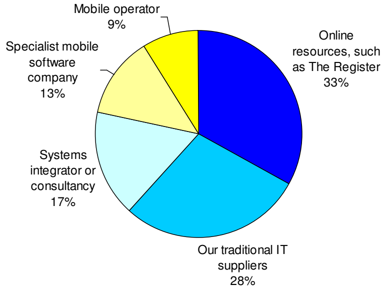


Experience tends to lead to increased confidence and a clearer view of which supporting technology might be useful to employ, but experience is not always close to hand.

When asked for their primary source of advice or guidance, over 50% turn internally to colleagues; however those who look externally first, turn mainly to online sources and traditional suppliers, and this undoubtedly reflects the general view for external advice (Figure 17).

Figure 17

Where do you expect to turn first for advice or guidance on the issues of mobile security, device management or mobile user support? (external sources relative to each other)



Too much reliance on internal advice means companies can become concerned about non-issues and miss out on learning from good practices and experiences elsewhere in the industry. Internal experiences should be balanced with a broad spectrum of views from suppliers and independent observers whenever possible.

7 Conclusions

Although the deployment of smart handhelds brings a new set of challenges, lessons can be learned from the good practices built up over years of supporting laptop users and from other areas where control is maintained over corporate assets and security (see Appendix A).

The complexity increases for smart handhelds with the diversity of device types and broader user community. There is no silver bullet to dealing with the challenges, but steps can be taken to minimise risks and keep costs under control, while still benefiting from the flexibility and productivity promised by remote or mobile access.

Done well with committed management support and user acceptance, smart handhelds and laptops can be deployed effectively, and provide benefits for both users and the business.

7.1 Acknowledgements

This kind of research is crucial to all of us in the business and IT community - suppliers and customer organisations alike. We would therefore like to thank all of those participants who contributed so generously, with patience and good humour, towards a better understanding of issues in this important area.

Appendix A – Bringing control and security to a diverse mix of mobile devices

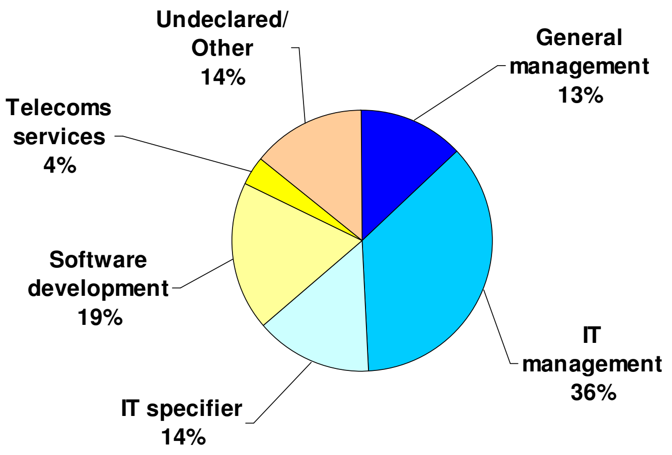
Organisations need to deal with the complexities of a diverse array of mobile devices, whether officially sanctioned or not. This check list serves as a reminder for those experienced in mobile device management or as a discussion document for those validating their concerns with a third party.

- **Establish policy**. Start with a business policy for mobile access, which feeds into a narrower IT policy. Set out in clear terms what the organisation plans to do, why actions should or should not be taken and how. Decisions are then aligned to business needs rather than the technology-de-jour. Policy is important even if there is no plan to officially deploy smart handhelds or laptops.
- **Communicate**. Policy must be understood from the top to the bottom of the organisation and implemented as business processes. These should be part of employee training, from the induction process, to regular ongoing communication say via an intranet site. Every user should understand the company policy, their responsibilities in the business processes including expected levels of care, penalties for misuse, and acknowledge their understanding and acceptance.
- **Build on experience**. Policy and processes need to adapt to changing technology, threats and usage patterns of mobile working. Use pilots to gain internal experience, but foster and make use of external relationships with suppliers and partners to learn, review and build best practices.
- **Support policy and processes with technology**. Not as is often the case, the other way round. Automated backup and data synchronisation reduces the need for user intervention and the possibility for errors. Over the air updates simplify device management ensuring that critical patches and security upgrades are deployed as soon as possible. Dependence on the over the air connection is a limitation, but it is a useful solution when impractical or uneconomic to 'return to base'.
- **Single point of support**. Users need a simple method of getting help or advice in the event of a problem. During a pilot, provide specialised support, but once deployment broadens, fold it into the standard support services. One number to call, one website to visit, one email address.
- **Protect the device.** Antivirus, firewall and VPN software protection should not be left to users, but provided as a corporate resource, installed on every suitable mobile device and updated regularly and automatically. If users provide their own devices, organisations should mandate licenses for protective software.
- **Asset tracking**. Log corporate assets given to employees in an asset register, update whenever loss, theft or upgrades occur and close when the employee leaves. This tracks the level of risk and instils responsibility to take care of corporate assets in users.
- **Amnesty.** If unofficial usage is already rife, offer an 'amnesty' with guidelines for what devices are acceptable, and how they can be brought into the corporate fold, rather than simply imposing an outright ban. Better to understand the size of the problem than ignore it hoping it will go away.
- **Limit choice**. An effective and simple solution is to limit choice. But first consider alternatives for different mobile requirements by running a number of pilots in parallel. Get involvement of a wide range of partners: handheld manufacturers for range and roadmaps, software suppliers for cross platform restrictions, and operators for connectivity options and limitations.
- **Keep a sense of perspective**. Total security and control of mobile technology is impractical and potentially smothers the productivity gains hoped for. Apply pragmatism, and weigh up the advantages against the risks and costs.

Appendix B – Interview Sample Distribution

Figure 18

Respondent by role



References

	Title	*Published*
1	IT Security – Bridging the Gap	Quocirca Ltd 2004
2	Enterprise Wireless Update – Scaling it up	Quocirca Ltd 2004
3	Mobile Email Momentum	Quocirca Ltd 2005

About Orange

Orange was launched in the UK in 1994 and has been at the forefront of innovation in the mobile world ever since, becoming one of the UK's leading operator with 14.2 million customers.

One of the world's largest mobile communication companies, Orange operates in 19 countries with 50 million customers worldwide and has services available in more than 140 countries across five continents.

Orange Business Solutions was launched in 2001 to service the UK business community. Now catering for all businesses, from the sole traders to multinationals, Orange has the fastest growing share of the business market in the UK. Internationally, Orange Business Solutions has over three million business customers worldwide and supports over half of the Fortune 100 companies in Europe

More information: www.orange.co.uk/business

About Quocirca

Quocirca is a UK based perceptional research and analysis company with 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 Morgan Stanley, Oracle, Microsoft, IBM, CA 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.

Most Quocirca research reports are available free of charge and may be requested from www.quocirca.com. To sign up to receive new reports automatically as and when then are published, please register at www.quocirca.com/report_signup.htm.

Contact:

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

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

quocirca