Quocirca Insight Report

January 2006

Mobile Security and Responsibility

Taking the right attitude to secure mobile technology

Contacts:

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

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

Orange Media Centre
Tel +44 207 984 2000

When companies extend their business IT operations to mobile employees, their risks are increased as valuable software, data and devices are taken out of the protected perimeter of the office, and placed in the pockets, pouches and briefcases of users. Business processes may run more efficiently, and employer and employee have more flexibility in how they conduct the working practices, but do both parties gives sufficient attention to their responsibilities? There is a tendency to believe that where there are challenges with a particular use of technology, the solution is to apply yet more technology, but this is of little benefit if the attitudes to its use are complacent or irresponsible.

KEY FINDINGS

- **Workplace flexibility is at least as important a driver for mobility as productivity**
  While efficiency and productivity are clearly important justifications for adopting new technology, workplace flexibility is the top reason for interest in mobile technology for three quarters of IT professionals. However, those companies that deploy the technology most widely are those with a corporate strategy for mobile working.
- **Mobile security policies are described as 'vital' but largely not well implemented**
  While the vast majority of IT professionals believe it is vital for security policies to cover the use of mobile, wireless or cellular devices, a third do not have such a policy in place. Although this is less for those with more widespread deployment, still one in five of those companies with broad deployments of both wireless laptops and smart handheld devices do not have effective policies in place for mobile security.
- **Users are recognised as a problem, with attitudes that are often irresponsible and careless**
  It is widely realised that mobile users create more challenges than the technology, and alarmingly, a significant percentage of companies think their mobile users have an irresponsible attitude to security, even among those with experience of broad usage.
- **Over-communication helps generate the right attitudes to user responsibilities**
  While intranets and emails are default ways to explain policy, many companies take advantage of two-way communication through training, employee induction and management. This is more pronounced for those with experience of larger deployments, and these companies are more likely to believe their users understand what they have to do and more likely to behave responsibly.
- **Many organisations are not setting the right examples**
  Most recognise that security is a shared responsibility between organisation and individual employee, but even where security policies are present they are not strictly enforced in over a third of companies. There is a lack of clear leadership from the organisation, and uncertainty as to whether employees in senior positions take security sufficiently seriously.
- **IT managers are cautious and pessimistic about the difficulties caused by mobile devices**
  While plenty of emphasis is placed on security, and most IT managers believe smart handheld devices should be protected by a PIN or password, a worrying one in five do not regard a mobile security policy as vital. Half believe mobile users have an irresponsible attitude to mobile security and although many users are given at least some choice of device, IT managers prefer to have a single corporate standard for everyone.
- **But general business managers optimistically tend to underestimate the problem**
  While most believe a mobile security policy is important, a third do not believe this to be vital, and are more likely to believe that users are responsible than do IT managers. They are twice as likely to allow users to choose whatever device they want, and would tend to leave it to individual users to decide whether they want to use a password or PIN on their device.

RESEARCH NOTE:
The primary research data upon which this report is based is derived from 2035 online interviews conducted in the fourth quarter of 2005 on behalf of Orange. Respondents were predominantly IT professionals, representing a mixture of supplier and end user organisations. Geographic location was specifically identified, with just under half outside the UK.

CONTENTS

1 INTRODUCTION **3**

2 CHALLENGES OF MOBILE SECURITY **3**

3 SETTING POLICIES **3**

4 USER RESPONSIBILITY **4**

5 INVOLVEMENT AND COMMITTMENT **5**

6 REALITY BITES **6**

7 CONCLUSIONS **7**

7.1 ACKNOWLEDGEMENTS 7

APPENDIX A – CREATING THE RIGHT ATTITUDE **8**

APPENDIX B – INTERVIEW SAMPLE DISTRIBUTION **9**

REFERENCES **10**

ABOUT ORANGE **11**

ABOUT QUOCIRCA **12**

1 Introduction

The safe and secure use of technology is a legitimate concern for any business, and this is often raised when considering the use of mobile technologies. Once systems or access then leave the office many problems may arise.

Increasingly smaller and more lightweight devices can be lost, forgotten or stolen with relative ease. According to a recent survey of Taxi drivers, thousands of laptops and many more mobile phones are left on the seats of Taxis in cities around the world everyday. How should a company address the security issues of small or mobile devices? Is the answer a technology solution or is it more about user responsibility?

This report examines the impact of user attitude on mobile security. 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, interviews were conducted in connection with a popular online news site. Of the 2035 respondents, 35% have broad experience of wireless laptops, 19% have broad experience of smart handhelds, with around a further 55% in each case having more limited or unofficial experience. For brevity, those with broad experience of all devices are described as committed leaders throughout this report.

2 Challenges of mobile security

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.

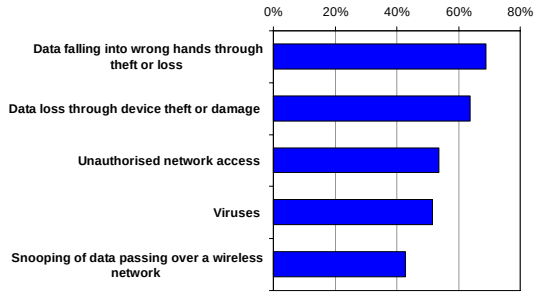
Smart handhelds are defined for the purpose of this report as handheld or pocket-able devices that connect to a wireless or cellular network, and can be installed with software. This includes networked PDAs and smartphones, and the report uses the term 'handheld' as an all-embracing term.

Both laptops and handhelds bring two challenges to IT: they carry information outside of the physically controlled systems, and offer remote access back to the protected environment.

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 only emerging with handhelds, previous research[1] shows that those with broad experience of both are more concerned with losing data (Figure 1).

Figure 1

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



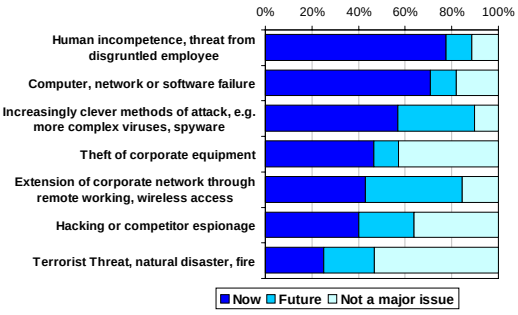
From 'Mobile Devices and Users' – Summer 2005

In many cases of data loss, the actions of the user leading up to the event will play an important part; was the device dropped, was it left unattended, or was it simply mislaid? How each user views their responsibility for the safety and integrity of the device will affect any attempts at securing its usage.

When Quocirca[2] explored general corporate data risks in 2004, remote or wireless access was not seen as the highest current threat, but the one growing most significantly in the future (Figure 2).

Figure 2

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 concerns surrounding corporate data 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.

While users cannot be held entirely responsible for virus or malware attack, their actions can affect the level of risk. If they are aware of the extent of the security challenges faced by the organisation, the consequences of a failure, and their own duty towards safeguarding corporate assets, they are more likely to adopt a more responsible attitude to mobile security.

3 Setting Policies

The starting point in any organisation is to establish what the company's business security policy should be, and how that will then impact on defining appropriate IT policy or procedures.

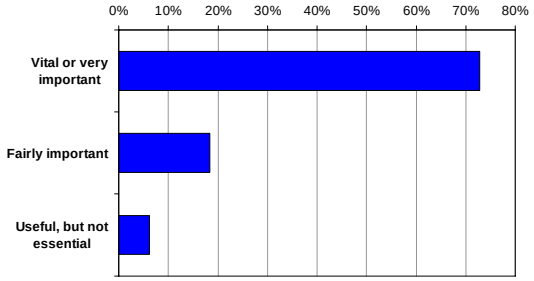
This is important whether the company plans to officially adopt the technology or not, since, as the cost of mobile technology products and devices is dropping and their capabilities are rising, users will bring them into the business unofficially or as personal tools.

Unofficial use occurs whether companies permit it or not, and should not be ignored. This happened from the outset with Personal Digital Assistants (PDAs), and has continued with smartphones, iPods and memory sticks. Companies should be aware, and set blanket policies to cover all types of technology not officially sanctioned.

As security is always a major IT concern and mobile devices of all types are proliferating, it would be reasonable that all companies should see the need for a security policy that covers mobile devices. However, small but significant percentage, do not see this as vital (Figure 3).

Figure 3

How important do you regard the need for a security policy to cover the use of mobile, wireless or cellular devices?

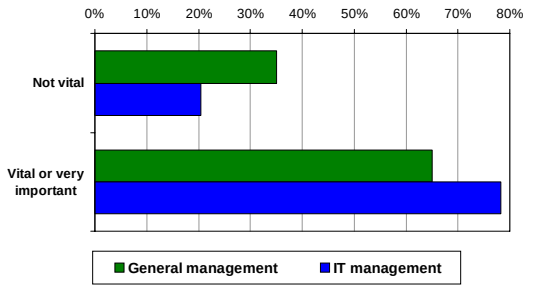


Looking closer at the figures reveals a greater concern. IT managers are more aware of the need for a security policy than those in general management roles, but even so, one in five do not see it as vital (Figure 4).

A much larger percentage of general managers have the same over-relaxed approach, and this is often reflected in the comments of IT managers who have to pick up the pieces after a failure. It should be a business imperative to take security seriously, and an IT imperative to implement and support that business imperative.

Figure 4

How important do you regard the need for a security policy to cover the use of mobile, wireless or cellular devices?



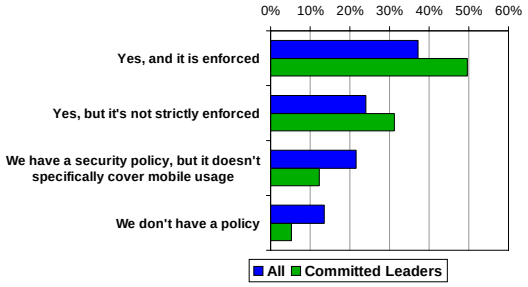
Even though four out of five see the necessity of a policy, only three quarters of these overall actually have a security policy that specifically covers the use of mobile technology (Figure 5). This may be due to a lack of experience, or time pressures, but it is best to define a mechanism to let all employees in the company know where they stand on security issues right from the outset.

Those with experience of dealing with the challenges of managing laptops, and emerging mobile devices, such as smart handhelds, the committed leaders, are, however more likely to have a policy in place.

Worse, there are too many who do not take the security policy they have seriously enough to keep it strictly enforced. This sets a bad example to users, and is likely to be one reason why user attitudes towards mobile security are often seen as careless.

Figure 5

Do you have a security policy that covers the use of mobile, wireless or cellular devices



Enforcement is not about punishing careless behaviour, although that should be taken as a last resort, otherwise it will not have the desired deterrent effect. Users must believe that a policy has teeth; otherwise any further communications about changes, improvements or responsibilities will simply be ignored.

Humans learn from childhood how to push the limits of what is, or is not permitted, and discipline with merely the threat of punishment goes a long way towards encouraging responsible attitudes.

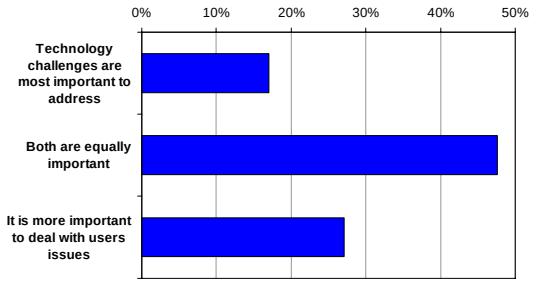
4 User responsibility

The complexity of many technology projects can create a tendency to focus more on the technical aspects of implementation than on the social and human aspects of usage. This approach can easily lead to the failure of a project, when the productivity and efficiency gains that were expected, evaporate when users find the solution is too complex, or does not fit well with their working patterns.

Getting users involved early, so their feedback can be heard, generates buy-in and increases the likelihood that users will understand their responsibilities. Most companies recognise that users' issues are as important as or even more important than the challenges from the technology (Figure 6). What they must ensure is that users feel like an integral part of the solution, not an afterthought.

Figure 6

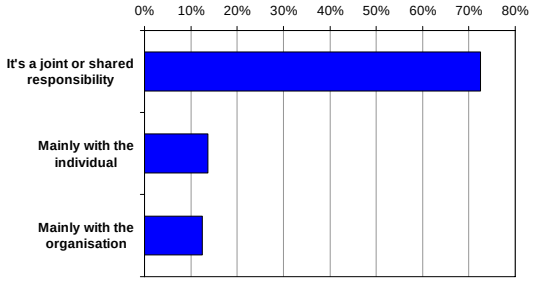
What are the key challenges for deploying mobile devices: technology challenges or those relating to users and the working process?



Increasing their commitment encourages users to take more responsibility for the mobile assets, both the device and the data on it. While most believe this responsibility is shared between the individual employee and the organisation, once outside the protection of office environment, the onus has to rest further on the individual (Figure 7).

Figure 7

Should the responsibility for keeping a mobile device and the data on it safe and secure lie with the individual user or with the organisation?



For its share of the responsibility, the organisation has a duty to equip the employee with the tools and confidence they need to operate securely.

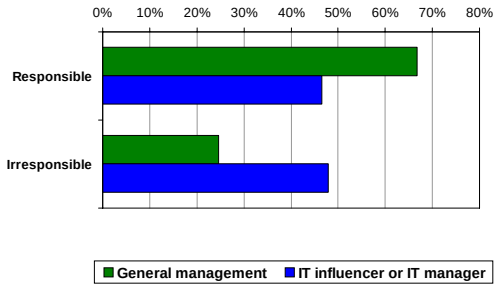
This can include smart technology to synchronise, lock, remote control or protect from viruses, but more importantly, users must be informed what to do in any situation where security may be compromised - who to ring, what to say or do, and how quickly to do it. This comes from acceptance and adherence to the code of conduct, outlined in the security policy.

Unfortunately the organisation also has to accept that failures will occur and mitigate the effects of a loss or a break in security. For the business this will include recovery procedures and ultimately insurance. For the individual concerned, there should be a process to discover what went wrong, check whether an employee was at fault, and take appropriate action.

This may be disciplinary or simply financial redress, but it has to be clear, consistent and anticipated by the employee. Line managers and personnel or HR departments play a major part in encouraging the right attitude, but in this area at least, it seems managers take an optimistic view of the attitude of employees (Figure 8)

Figure 8

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

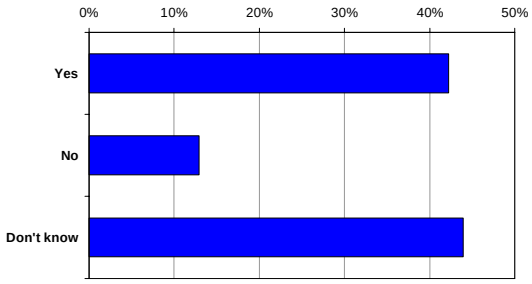


Those involved in the IT processes of deploying and managing the use of mobile devices, recognise the problem most often lies with user attitudes. Users are seen as "lacking in common sense" or "careless" while managers are "cavalier" or "ignorant" about the impact of security threats and fail to punish persistent offenders or violators of security policies.

Clear leadership and a consistent approach is important. No matter what the level of seniority of employee, each is responsible for the organisation's security. Some responses noted that senior management set a "very poor example", and although many believed the person responsible for setting security policy took precautions for securing their own mobile device, many were unsure (Figure 9).

Figure 9

Does the person responsible for setting security policy in your organisation (e.g. IT director/CIO, CEO) protect their smart handheld mobile device with a PIN?



It is better for senior managers to be open and public about their support for security measures, rather than quietly abiding by them. This support must be real, however, and it would be a disaster if someone supporting a strong security policy was found out to be flouting it themselves.

5 Involvement and commitment

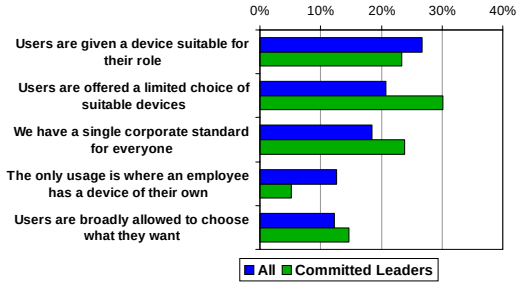
Although many users build strong personal attachments to the mobile devices they have, these are, after all, business tools for improving working processes. Allowing users complete freedom to choose their own devices may satisfy their desire to carry the coolest gadget, but it will make the task of device management and security, much harder.

Giving users no choice whatsoever can be a hard rule, and must be applied consistently as a corporate standard. Better still is to give some, if only limited, choice as this will

increase user buy-in, and ensure that the right tool is available for the right task. This is the approach most often adopted by the committed leaders (Figure 10).

Figure 10

Typically, how involved are users in the process of selecting what type of mobile devices they will use in their job?



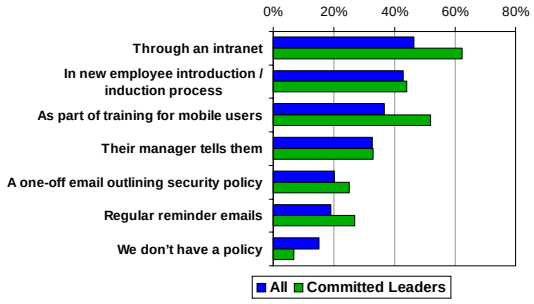
It is important that users understand why decisions have been made to limit choices, especially if there is only a single corporate standard. While they might favour one make of laptop over another, or have aspirations of using a particularly fashionable smartphone, most will prefer continued fulfilling employment with a profitable company offering rewarding salaries over one that is spending more than is strictly necessary on technology.

As well as the decision processes which lead to the definition of policy, users need to be made fully aware of the policy itself. This has to be done early and ideally at the key start points – when the employee joins the company, and when they accept a mobile device or devices (Figure 11).

The importance of specific training is especially noted by those with broad experience of deploying mobile devices. Although many users could indeed find out how to make use of devices from manuals, a formal program of training ensures that best practices can be shared, and the responsibilities of security and good mobile communications etiquette can be understood. This reduces the potential for misunderstanding and problems later during usage.

Figure 11

How are users made aware of the mobile security policy?



As mobile security policy is something that is likely to change markedly over time when new devices or solutions emerge, or new threats are identified, this awareness must come as part of ongoing communication.

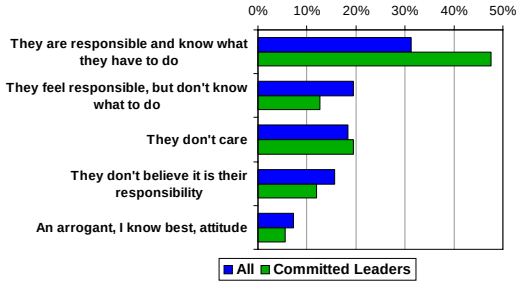
Again the committed leaders with experience recognise the need to target communications with the mobile user closer to their point of need, sending reminder emails and presenting it on the intranet. It is important that this information is not hidden away, but displayed or linked prominently. It is also important to ensure that support lines are clear and simple, with a single support number or email address to be used in the event of a problem.

6 Reality bites

Despite the best efforts of those with broad experience of both laptops and smart handhelds, it is clear that a challenge remains. Committed leaders take communications with users and their education seriously, and it does increase their level of responsibility (Figure 12).

Figure 12

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



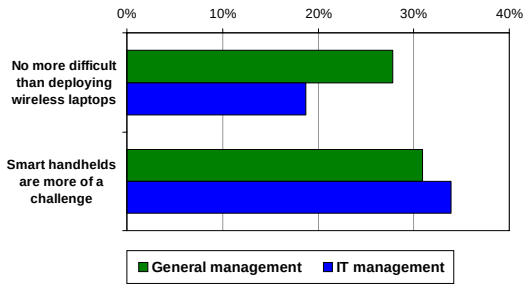
However, even here over a third of users have a poor attitude, and behave carelessly or arrogantly with mobile technology. While effective communications have made users more aware of what they have to do, it has not substantially improved their acceptance of responsibility.

The attitude of management plays a key role in influencing employee behaviour. The punitive side of this is to enforce policies with penalties for failure to comply, or by passing some of the financial burden of replacement after irresponsible actions, but this is already after the event.

Better to treat the whole process of mobile deployment, and the devices themselves as a serious part of extending the business, and not simply the allocation of a few flashy gadgets to an elite few. Line-of-business managers generally underestimate the complexity of this challenge more than their IT counterparts (Figure 13).

Figure 13

How does the challenge of deploying smart handhelds compare to deploying wireless laptops?



Taking the process seriously means that users have to feel they are being entrusted with something important, that will

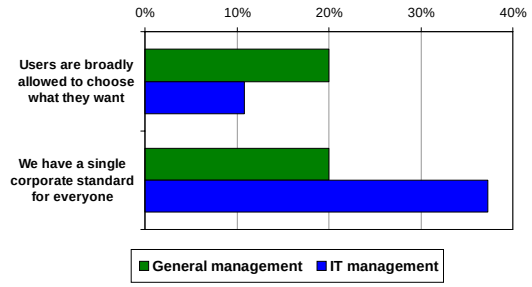
be of value to them in their working role or career, and be worthwhile for the business. This means:

- involve them early to gain feedback and buy-in
- tailor to the needs of their role
- set understandable standards and policies
- provide training ahead of implementation, not after
- offer full support during the process
- get feedback afterwards to refine

Taking an interactive and consultative process with users does not mean bowing to their wishes, and organisations need to set standards. However there is a danger that different decision makers will take a more simplistic view – managers wanting an easy life will allow too much choice, IT managers for a similar reason will want to limit to a single standard (Figure 14).

Figure 14

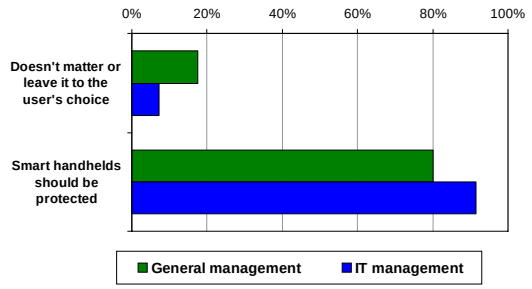
For committed leaders – Typically, how involved are users in the process of selecting what type of mobile devices they will use in their job?



Both IT and line managers need to understand the issue as getting user buy-in is critical to the security process. From earlier Quocirca research[1] it was apparent that even those with broad experience of smart handheld deployment had a more lax attitude to the security of these devices than laptops. Although confirmed usage of PIN or password protection at senior levels is less than clear (Figure 9), hearts are mainly in the right place, at least for IT managers (Figure 15).

Figure 15

For committed leaders – should smart handhelds have a PIN or password?



Once again, general business managers have a more lenient view of users in general, and from IT management observations, this may very well be because so many managers have a lax approach as users themselves.

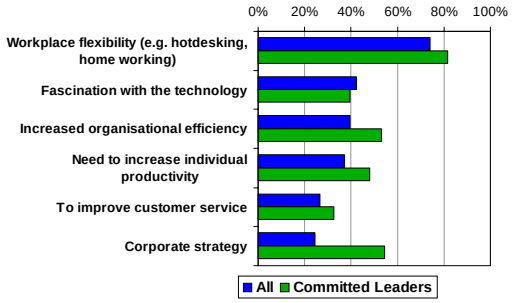
7 Conclusions

Decisions can be driven by a fascination with the technology for the latest 'toy' or 'cool gadget' rather than something suited to a business need. This means the impact on technology infrastructure and human working processes tend to be pushed to one side.

The question to address is a simple 'why deploy mobile technology at all?' Where a business case can be made, suitable technology will provide a return on investment, but the driving forces are generally more complex than a simple productivity gain (Figure 16).

Figure 16

What is driving the interest in mobile technologies?



However, security is often the largest obstacle to progress, and this is massively influenced by user attitude as well as the technology infrastructure. In many ways the arguments are difficult to rationalise as the impact of security breaches or failures are difficult to comprehend, especially to those outside the IT discipline.

The business potential for increased workplace flexibility and productivity or efficiency can only be realised if users are fully committed to the process. This commitment has a double benefit. Not only does it help ensure that expected productivity gains materialise, but it also adds to the integrity and security of the solution.

Both IT and business managers can gain benefit from this, but each in their own way has to accept the validity of the views of the other, and find a compromise that takes neither a too optimistic, nor a too pessimistic point of view.

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 – Stimulating a Responsible Attitude

Even companies with well thought out policies and well implemented solutions need to generate the right attitude and approach to security among their users. 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.

- **Sensible policy**. Ensure that the security policy is based on good business sense and a rationale that can be justified as a means of protecting the assets of the business, operating in the best interests of employer and employee.

- **Engage users with consultation, not prescription.** Communicate early with potential users and their representative bodies, create trust and expect responsible behaviour. Demonstrate the security challenges the business faces, the measures the organisation will put in place to tackle them, and how they as users are expected to play their part.

- **Fit solutions to user and business needs**. Technology can be used to support the needs of the business and still be adapted to the more individual needs of users. Forcing the adoption of one solution across a mix of needs or use cases will be counter productive.

- **Train before, support during**. Do not leave anything important to be found out, discovered, or decided upon by individual users. Run comprehensive training, use workshops and participation to establish best practices and etiquette that users can buy into. During and after deployment ensure that users are kept informed and updated with any matter concerning mobile policy and that they have a simple and straightforward route for getting support.

- **Lead from the top**. Not only from the top, but everywhere. Be consistent in the application of policy, from the options available to the rules enforcing security. Do not make exceptions for senior or more experienced staff. They may or may not be less of a risk, but they are the most visible role models.

- **Enforce.** Policies must have teeth to be effective, and there are times when rules must be enforced. Consequences must be clear and understood from the outset, so that violators are neither surprised nor feel aggrieved. As with any form of disciplinary practice, enforcement should scale according to severity and frequency of the problem.

- **Keep a sense of perspective**. Not everyone will be sufficiently responsible or have the right attitude to support the organisation's security policy. Ensure that a safety net of measures are in place to deal with the most likely eventualities – backup, contingency and insurance all have their part to play. Apply pragmatism, and weigh up the advantages against the risks and costs.

quocirca

Appendix B – Interview Sample Distribution

Figure 17

Respondent by role

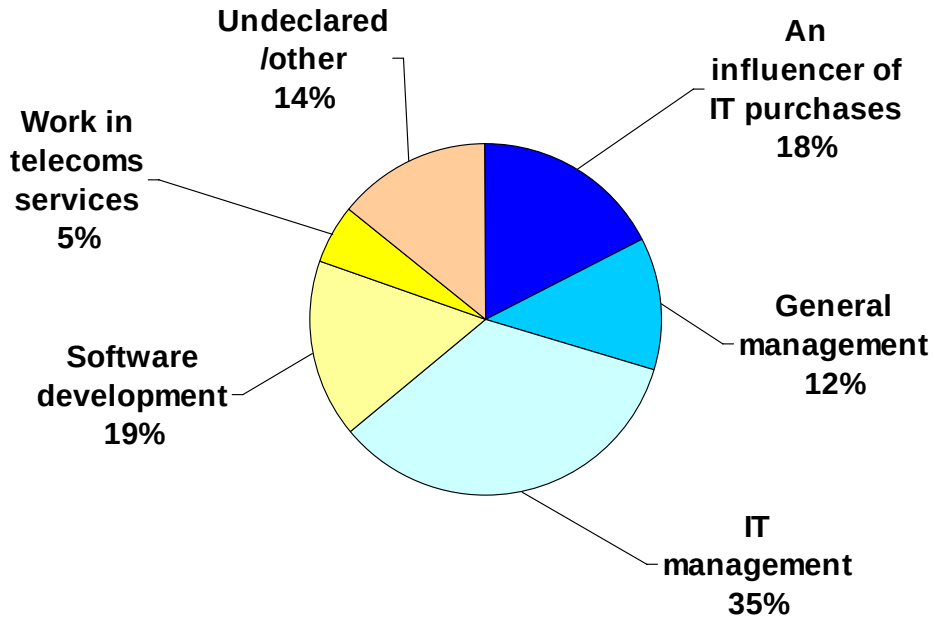
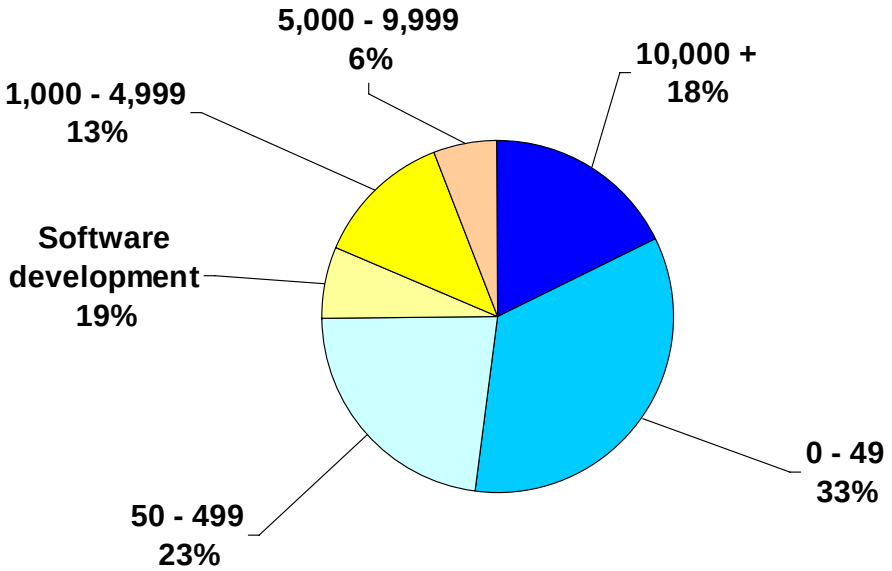


Figure 18

Respondent by Company Size



References

	Title	*Published*
1	Mobile Devices and Users	Quocirca Ltd 2005
2	IT Security – Bridging the Gap	Quocirca Ltd 2004

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, Vodafone, Oracle, Ericsson, Microsoft, Orange, IBM, O2, 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