

Securing the Enterprise

Managing the challenges of mobile communications

Contacts:

Rob Bamforth
Quocirca Ltd
Tel +44 7802 175 796
rob.bamforth@quocirca.com

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

In the competitive global marketplace, businesses are placed under increasing pressure to have a flexible and efficient workforce that is as productive as possible and reacts to customer demands and changing conditions. The mobile phone, laptop and other small smart devices for mobile connection to corporate data all support these needs, allowing access wherever required to fit business processes. This brings its own risks, but businesses depend upon the flexibility delivered by their increasingly mobile and dispersed workforce, so must adopt a positive approach to securing their intellectual and physical assets as well as their employees.

There are many aspects which are explored in this paper in greater detail, but the following list provides a mobile security action plan for an organisation of any size that is aware of existing use of, or has plans to deploy and take advantage of, mobile technologies.

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.

- **Establish sensible policy.** Start with business needs, feeding them into the IT plan. Ensure that the security policy is based on good business sense that can be justified as a means of protecting the assets of the business, operating to fit within day to day working practices. Policy is important even when there is no current plan to officially deploy mobile technology.
- **Engage users with consultation, not prescription.** Policy must be communicated throughout the organisation and implemented as well understood business procedures. Involve users early to create trust and expect responsible behaviour in return. Demonstrate clearly the security challenges faced, the measures being put in place to tackle them, and how user responsibility plays its part.
- **Choice and Amnesty.** Offering some choice will generate user buy-in, but keeping it to a minimum will lower support costs. If unofficial usage of mobile devices to access corporate data is already rife, offer an 'amnesty' with guidelines for what is acceptable, and how it can be brought into the corporate fold, rather than simply imposing an outright ban.
- **Automate security processes with technology.** Scheduled backup and data synchronisation reduces the need for manual 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. Network dependence is a minor limitation, and is more practical and economic than having to 'return to base'.
- **Actively engage with all partners and suppliers.** Find out about default settings, available security options and future plans from laptop or handset providers and from existing network or system management software suppliers. Investigate connectivity options and limitations, and how far network operators and service providers will go in providing outsourced or hosted security services.
- **Protect the device.** Antivirus, firewall and VPN software protection must be installed on every suitable mobile device, updated regularly, and include users' own devices. Known connection risks such as Bluetooth and Wi-Fi must be properly configured. Register mobile corporate assets given to employees, update whenever loss, theft or upgrades occur and when the employee leaves or the asset is returned. Ensure data removal upon termination.
- **Train before, support during.** Run comprehensive training, use workshops and participation to establish best practices and etiquette that users will buy into. During and after deployment ensure users are kept informed and updated with any changes and that they have a simple and straightforward route for getting support. One number to call, one website to visit, one email to address.
- **Enforcement.** Policies must have consequences to be effective, and there are times when rules must be enforced. These must be clear and understood from the outset, so that violators are not surprised. As with any form of disciplinary practice, enforcement should scale according to severity and frequency of the problem.

CONTENTS

1.	INTRODUCTION.....	3
2.	DEFINING THE THREATS	5
3.	SETTING OUT POLICY.....	8
4.	USER ACCEPTANCE AND RESPONSIBILITY	10
5.	SUPPORTING POLICY WITH TECHNOLOGY	13
6.	BROADER GOOD BUSINESS PRACTICES.....	16
7.	CONCLUSIONS	17
	APPENDIX A –.....	18
	ABOUT ORANGE.....	19
	ABOUT QUOCIRCA	20

1. Introduction

At one time information technology was kept locked in data processing centres run by a small number of specialists, with access strictly controlled by physical security. That changed forever with the mass availability of personal computing power through the PC, and the widespread availability of connectivity through the Internet. Business telephone communications once constrained to a limited number of desk phones now extend to the ubiquitous mobile phone, containing contacts, voicemail access, messages and diaries.

Companies are extending more of their business IT and communications operations to employees outside the bricks and mortar of the office, increasing the level of risk as valuable software, data and devices are taken out of the protected physical perimeter, and placed in the pockets, bags and briefcases of users. Today this is more often a major strategic imperative, rather than an ad hoc or one off deployment and with the serious and expensive nature of such investments, care should be taken to ensure all aspects are well thought out.

Securing mobile communications and remote access technology outside the office brings many challenges. The physical barrier is bypassed, and with many ways to communicate, both with and without wires, the electronic access points are many, each with their own vulnerabilities. These are compounded by the shrinking size of all manner of mobile devices which can be lost or stolen with relative ease.

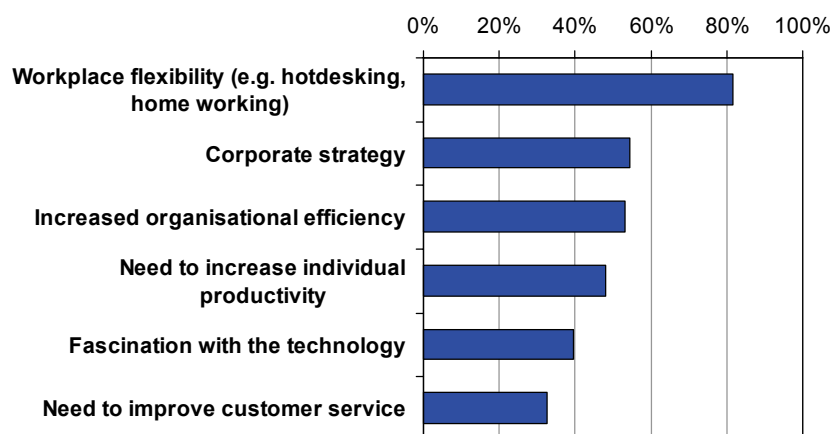
At one time mobile technology might have been limited to a mobile phone only containing a few contact details, and a floppy disk capable of storing the odd document. Now, gigabytes of data can be carried on a memory card the size of a thumb, mobile phone handsets can transmit megabytes of data anywhere in the world in a matter of seconds, and entire businesses including their entire customer databases and accounts can be run on a small laptop computer.

Mobile technology is delivering many benefits, with a shift in the usage and emphasis of IT (Figure 1). Business processes run more efficiently, while employer and employee have more flexibility in how they conduct the working practices, bringing balance for the individual and productivity gains for the organisation. Employees are able to simply and immediately make contact with their colleagues, with their customers or suppliers, and outside work, with their social groups.

This flexibility brings with it responsibilities for employer and employee, and this white paper examines the security issues arising from mobile access to IT and communications and how businesses can nurture good practices for their organisation and their staff. The paper outlines the issues and offers some guidance to those facing the challenges of security in a mobile context and draws on findings from discussions with industry suppliers and businesses, but also on specific research conducted into end user and management views of mobile security. This included online interviews with professionals in a wide range of organisation sizes and industries.

Figure 1

For those deploying it, what is driving the interest in mobile technology?



From 'Mobile Security and Responsibility' – January 2006

Information and resources have always been more at risk when outside the office, but what has changed is the volume of data travelling beyond the perimeter, the number of employees with access and the speed at which the resources can be lost, copied or

stolen. The other major change is a shift in consumer access to technology. At one time new technologies gained a foothold among business users, before reducing in cost sufficiently to become consumer purchases. Now, products often move in the other direction. Employees have access to more and better technology at home than they have in the office. This leads to a more relaxed and confident approach to technology, which can border on irresponsible, and the risk that consumer products are being brought into the office environment outside the control or knowledge of the IT department or business management.

Overall, both organisations and the individuals they employ have to take mobile security seriously, while still ensuring they can take advantage of the benefits. At a strategic level this means the organisation must do its utmost to set out the intent of securing its business processes and resources in the form of a policy, and ensure that this policy is well understood by all those it affects. Tactically there is a need to give sufficient resources to internal departments, such as IT and personnel, so that they support the policy with tools and procedures to implement it effectively and efficiently.

Clearly no single plan will work for all, and the strategy should be adapted to meet the specific needs of companies and organisations of all sizes and types. There is no point taking too restrictive an approach, as that would defeat the object of gaining benefit from the use of the technology. Neither is it acceptable to assume there is no challenge to address. It is most important to recognise that mobile technologies are becoming a fundamental part of our everyday world, and the impact on working processes cannot be ignored.

2. Defining the Threats

The first objective in securing any organisation is to define what resources need to be protected, and identify the range of threats faced so that appropriate measures can be put in place. The use of mobile technology exposes a number of business resources that need to be considered:

- The mobile devices, laptops and handsets themselves
- Data in transit
- Data stored on the mobile device
- Network capacity, connection or services
- Core IT infrastructure and applications
- Mobile business applications or software
- The employee themselves

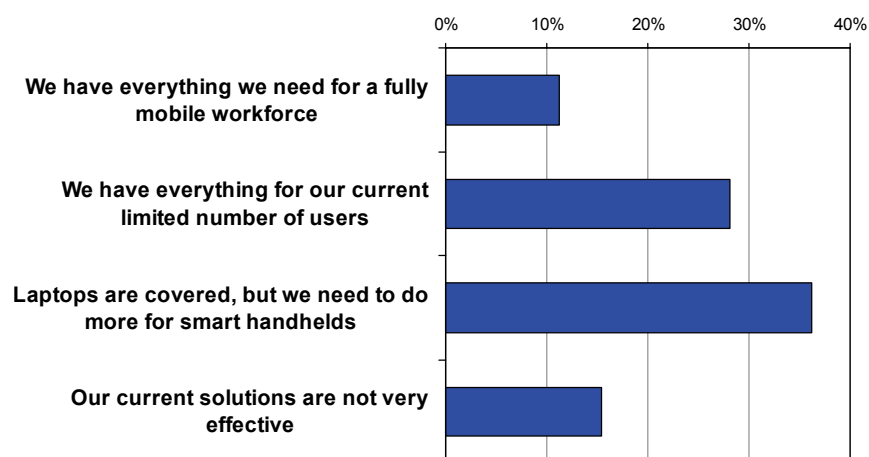
These resources are vulnerable to a different range of threats from both beyond and within the office boundaries. Once outside the office, the most significant means of protection of corporate information – physical isolation – is lost, but arguably even inside the office this shouldn't be taken for granted. Rogue wireless networks can be installed inside the building, or unprotected networks could be snooped from just outside.

The security risks for any organisation come from internal as well as external sources. These could be due to the deliberate or accidental acts of employees, or failures in business processes. External threats vary from those that are not direct attacks, but threaten the resilience of the business – terrorism, weather disruption or communications breakdown – to those that are malicious or deliberate acts for financial gain, sabotage, notoriety or a prank – stealing, spying and hacking.

As with any use of IT, mobile technologies share a common set of electronic threats from hidden software that behaves erratically, inappropriately or maliciously – viruses, worms, Trojans, spyware – to those attempting to gain access to resources they should not have – access violation, snooping, identity theft. This has been well understood by those deploying the traditional mobile extension to IT, the laptop, but as smaller mobile devices become smarter and more sophisticated these challenges have appeared on other platforms, and now need to be addressed (Figure 2).

Figure 2

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



From 'Mobile Devices and Users' – Summer 2005

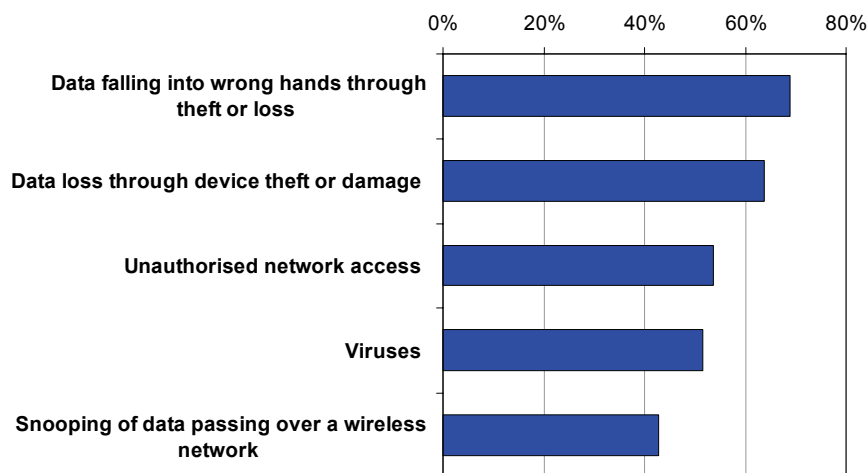
The onus is on the organisation to keep mobile security processes as simple as possible to accomplish the level of security required. This means identifying where security needs to be tight, and where it can be relaxed, and to distinguish how policy or controls should be applied.

For example those working in specified roles may be granted access to tightly controlled information, but this access may only be available while those employees are in the office, or using what is known to be a trusted mobile device and connection. Or employees granted the use of a mobile email device may be compelled to always have a PIN in place to control access, but those with limited function mobile phones with, say, international calling barred, may be allowed to use the device without a PIN. The policy needs to be adapted to match the risk to, and the value of, the resources being protected.

Unlike the fixed assets of an organisation, which are physically protected inside the corporate perimeter, mobile technologies are more vulnerable to loss or theft, and this is a risk that is greatly influenced by user behaviour (Figure 3). Mobile technologies by their nature are used in environments where the pace is likely to be more hectic, so speed and simplicity is essential. Users will be more inclined to take short cuts, and anything that slows the process down is likely to be rejected or avoided. Even using PINs and password to access frequently used features may be seen as a burden, and switched off, given the choice.

Figure 3

What are the most important mobile security issues for those with broad experience of deployment?



From 'Mobile Devices and Users' – Summer 2005

Mobile devices and the use of IT and communications outside the office increase the scope of the challenge to those managing security as they offer more connectivity options for valid users or entry points for unauthorised users and malicious software, generically known as malware. Today's mobile employees have many different ways to connect their devices and any number of services available, each is potentially vulnerable.

- **Bluetooth** – This is susceptible to relatively short range probing for information, and many users leave their Bluetooth switched on, needlessly sharing information which at minimum could be the name they have given their phone. Even this could provide some useful information for mounting a social engineering attack. Bluetooth threats are also based on closed proximity, allowing devices to be surreptitiously contaminated by a passer by. The first malware noticed on mobile phones, the Cabir worm, used Bluetooth as transmission mechanism, and is still in widespread circulation today, although its adverse effects are more inconvenient than dangerous.
- **Wireless LAN, public Wi-Fi.** This can easily be mis-configured exposing access points or devices vulnerable to attack. With Wi-Fi now built into the core feature set of modern laptops and many mobile PDAs, those which are unprotected can be exploited as an ad hoc access point by those in the know. Wireless LAN security standards have been historically poor and are still maturing. If not all mobile platforms deployed by an organisation support the latest and most secure standard, some may risk using a less secure lowest common denominator.
- **Mobile data – GPRS, 3G, HSDPA** – The core networks are generally well protected by the encoding employed by service providers, but applications sending sensitive data will want to increase their protection as some of the network journey will probably be over a public network like the Internet. Additional layers of encryption, such as applications using Secure Socket Layer (SSL) or using a Virtual Private Network (VPN) to protect all traffic between the device and core service will be required for greater security.
- **Synchronisation** – As well as the wireless connection methods, many mobile devices will connect via a data cable or cradle directly to a desktop PC. This could be a route to infect the mobile device, but far more likely to be a potential route for mobile devices to bring malware in to infect the PCs on an internal network.
- **Email** – Business users are increasingly relying on their mobile email devices. For many this is a separate device to their mobile phone, and something else to mislay, or forget to protect with a password or PIN. Mobile email whether accessed from

a handheld device, or webmail account through a browser, needs to be protected. Any use of a third party device, such as a PC in a cyber café, or a laptop using third party network in a hotel should be treated as insecure, and information snooped either in transit, or by logging keystrokes.

- **Instant Messaging** – Although business use of Instant Messaging (IM) is not very widespread, many users will already use it for personal communication. It is vulnerable to the transmission of malware, and unlike email systems, instant messages are not likely to be being recorded. The availability of un-monitored IM with access to users outside the business could be a significant risk for sensitive data.
- **Voicemail** – Access to voicemail services should be protected by a PIN, but too many users either do not realise, or leave it set to the original default value for convenience. Those leaving sensitive messages on voicemail should always be aware that they may be listened to by someone other than the intended recipient.
- **SMS** - Although a managed service while in transit, service levels and message delivery are not guaranteed. Messages stored on a device can be easily accessed if the phone is stolen, and can often be recovered even when the user believes they have deleted them.
- **MMS** - These multimedia messages can carry executable programs which may contain a virus, or can be used for a sophisticated scam imploring the recipient to take some bogus action. MMS has already been used as a transmission mechanism for the mobile worm CommWarrior, which infects Symbian Series 60 based devices.
- **Memory cards.** Computer viruses were once transported on floppy disks, and the modern day equivalent is the memory stick or data card. A practical mechanism to transfer information quickly and easily between many types of devices, but could be a delivery route for malware or a way to extract precious or secret data, however email and other messaging applications are still the most common ways to deliver viruses.

At least with the second and subsequent generations of mobile telephony the cellular radio connections are relatively secure, as data is encoded whilst in transit, and access to cell tower and network infrastructure is controlled in the best way possible, through the commercial interest of the operators. However here the vulnerability lies as always at the weakest point, with the end user.

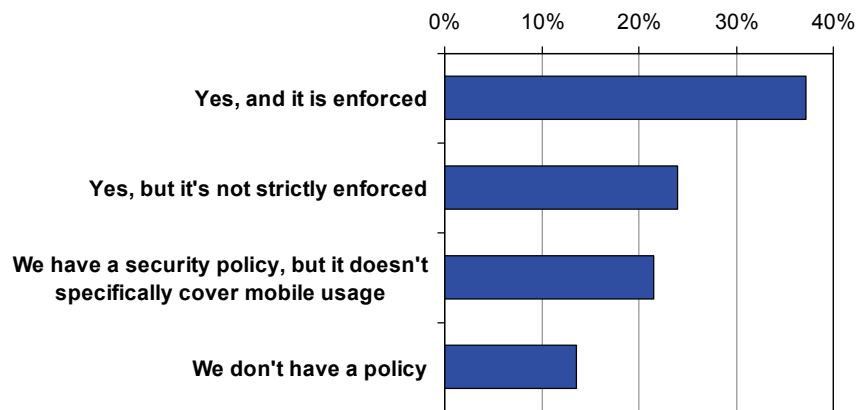
While the risks may seem endless, everything in life, especially commercial life is risky, and it is important to take a pragmatic view balancing risk with reward. For this reason the approach to dealing with the risks of mobile security should start with looking at the business, and defining a policy that starts with the business needs, and cascades these down into a security policy that addresses the risks with the appropriate level of educational, technical and financial protection.

3. Setting out policy

What is a mobile security policy? It should not need to be an overly complex and lengthy document that once written sits on a shelf unread and unchanging. A good mobile security policy should be well read, easy to understand, fit the business needs and be actively employed (Figure 4). After all, the objective of the policy should not be to prevent an organisation from taking advantage of technology that might be commercially beneficial, but to ensure that it does so in a way that can be made safe and secure. So the starting point in any organisation is to establish what the company's overall business security policy should be, how that then impacts on defining appropriate IT and communications policy or procedures, and in this instance how that should specifically be applied to mobile technologies.

Figure 4

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



From 'Mobile Security and Responsibility' – January 2006

All companies need some statement concerning employee use of a particular aspect of technology. This is important even if the company has no official plans to adopt the technology, since, as the cost of deploying mobile technology products and devices drops and their capabilities rise, 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, personal music devices containing hard drives and memory sticks. Where there may be a security issue, companies should be aware, and set broad policies based on appropriate user behaviours to cover all types of technology not officially sanctioned.

Security policies will always be a compromise between securing and protecting an organisation's assets on the one hand, and providing the mechanisms to openly liberate and exploit those assets for positive commercial gain on the other. Getting the balance right will depend on the attitude to risk, which might in turn depend on the size of organisation and industry sector. It is dangerous to ignore the risks exposed by any resource used by an organisation, and clarifying the approach need not be difficult.

A mobile security policy can be a short document that simply and clearly identifies the organisation's approach to security, and only really needs to outline the following:

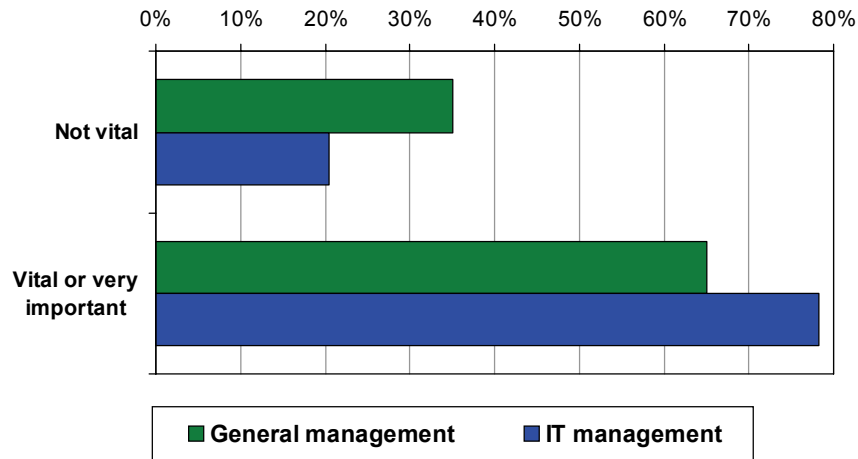
- **Objectives** - What is the policy for, why is it necessary, what does it set out to achieve.
- **Scope** - Who is included, what types of devices are covered – mobile, laptop, portable storage such as memory stick, CD, personal media players – and what types of information or access. This should also identify any personal/business overlap.
- **Responsibilities** - It is important that employees realise and understand their role in ensuring security, and how the organisation will support them. This must be clear and unambiguous, with the organisation leading by example.
- **Consequences** - There is no benefit in creating a blame culture, but everyone must understand that the policy is serious, with repercussions for breaking the guidelines laid out, which will be enforced with action taken to encourage appropriate responsibility.
- **Emergency Response** - As part of overall risk management and business continuity planning there should be simple clear direction of what to do if security is breached.
- **Further information** - Details on specific procedures and tools will clutter any policy and are likely to change regularly. This should be provided as references rather than embedded in the policy.

- **Review Process** - While the policy should be as stable as possible, it will not be set in stone, and must adapt upon occasion to changing business needs and circumstances.

This defines an approach which then needs to be understood and acted upon by all parts of the organisation (Figure 5). Some will be providing tools and resources to support the policy; others will be using it to help them go about their work. All have responsibilities to behave in a professional manner to support the security and integrity of the business.

Figure 5

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



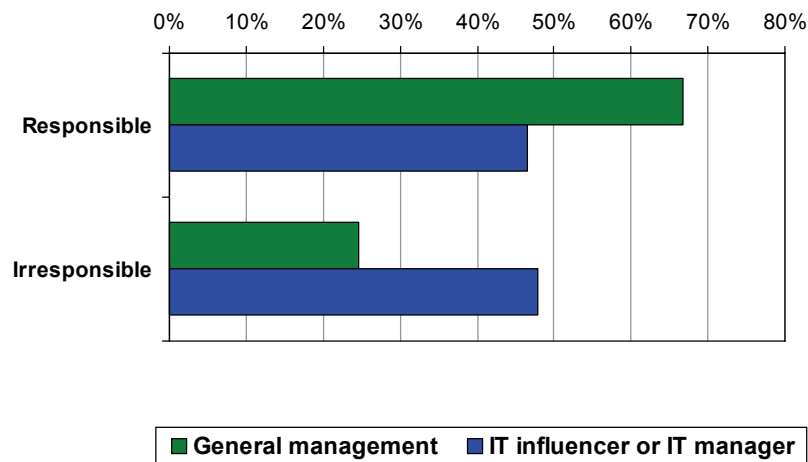
From 'Mobile Security and Responsibility' – January 2006

4. User acceptance and responsibility

Defining policy is only a starting point, and generating awareness and understanding of what this means to each and every employee is the next objective. Many of the vulnerabilities inherent in mobile technology come from the care, or lack of it, taken by the user, and much will therefore depend on their attitude. Encouraging users to behave responsibly and look after the corporate assets in their care forms part of the evolving etiquette for the mobile use of technology. This goes beyond direct security concerns into the good manners of paying attention in meetings rather than glancing at a laptop or handheld screen and the awareness of others in public spaces where too much information may be inadvertently disclosed. Those at the sharp end of dealing with security, the IT department, take a more negative view of user responsibility than those in management positions (Figure 6).

Figure 6

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



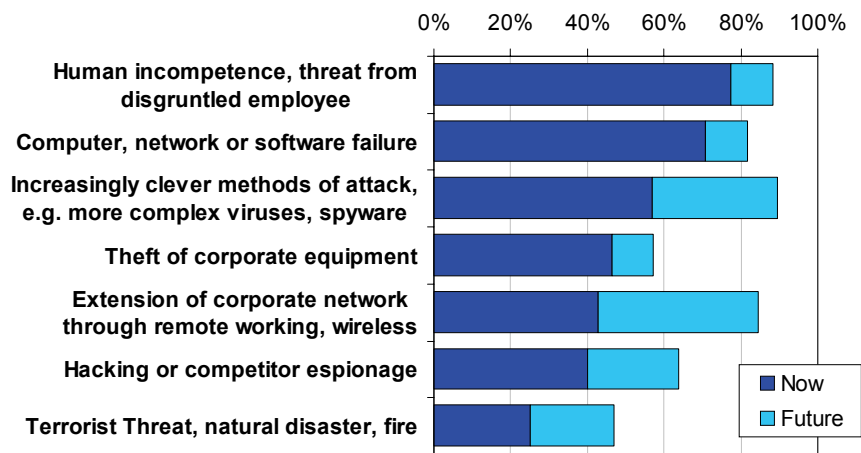
From 'Mobile Security and Responsibility' – January 2006

This may partly be the natural cynicism of the IT community, but also demonstrates the faintly rose-tinted view of those in management, who seem to be as lax as their charges when it comes to taking care of mobile devices. There have been a number of high profile stories in the media about laptops going missing, the BlackBerry of a senior executive being bought on eBay, and the data from the hard drives of de-commissioned PCs turning up in other countries.

The regular upgrading, replacement and hand-me-down approach to many mobile devices from phones to laptops poses a real risk. Data thought to have been deleted by one user can be unearthed with fairly little effort by a subsequent user of the same device, and this has been at the heart of many media reports. It may sound like a collection of apocryphal stories, but in reality it is likely to be an underestimated problem, and users are the weakest link (Figure 7).

Figure 7

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

If a user sees the security measures they are asked to undertake as a major drain on their productivity for no real purpose, they are likely to try to find ways around them or ignore them. If they are a slight inconvenience whose purpose is understood and appreciated, they are likely to use them. Gaining this understanding is not a one-step process, but requires sustained effort on the part of the organisation:

- **Buy-in** - Involve the users early in plans to deploy or use mobile technology. They are the ones who understand how their working processes really operate, and if new technology does little to help them, they are unlikely to take to it productively, or look after it.
- **Training** - Start just before anything is deployed so the information is timely and fresh, then continue with periodic training updates. Training should be seen as positive and career enhancing rather than a chore to be endured, so the style, length and delivery mechanisms need to be suited to the material and recipients. Induction training for new employees is a perfect time to start the process.
- **Common sense practices** - Define and publicise simple good behaviour through examples. Repeat and reinforce the message over time. Partly this comes from setting good examples elsewhere in the organisation, and partly it comes from listening early to user concerns. It is always possible that exceptions will have to be made, but the reasons behind these should always be well understood to avoid undermining the broader adherence to the policy. Managers should be seen to be supporting the policy and providing positive encouragement to those taking the right precautions.
- **Choice and restrictions** - While IT managers might prefer to limit choice to a single corporate standard, having a bit of input and choice is very important for end user buy-in. Different form factors may have a better fit on their task needs, but also personal choice will give a feeling of ownership, and therefore commitment to take care. Clearly a completely open selection process would be problematic, and costly with little opportunity for economies of scale, but a limited choice would give users a positive view of the technology they are being asked to carry for their work. This is particularly important when it makes inroads into their personal as well as business life, as mobile phones, and other smart handheld devices, often do.
- **Upgrades** – This is a particularly controversial problem area, especially where technology is advancing rapidly. New mobile devices with improved features may seem like the right logical step to the user, but are likely to introduce new problems for the IT and communications management, as well as increasing costs. If there is too easy a route to have devices replaced with the latest model, it might be abused. Nobody likes having last year's phone, if a new one is out, but organisations need to apply controls to any upgrade process to avoid devices being 'accidentally' lost or broken.
- **Support** - The easier it is to report a problem, loss or theft, the more likely a user is to respond quickly and effectively. Have a single helpline number or contact point, do not create new or separate channels to specifically support mobile users, put the call routing intelligence in the helpline, rather than something the user has to work out. Where possible give alternative paths to access the contact point – email, web, phone – rather than assuming the user has access to one particular method. It will be far easier to report a stolen laptop over the phone than by a web form or email and to report a stolen phone using a web browser.
- **Amnesty** - It has to be recognised that mobile technology is complex, diverse and evolving. There needs to be a way for a security policy when introduced, or amended to take into account existing conditions. If users have used or provided their own technology, for example PDAs first entered the workplace as employee-owned devices, these need to be brought into line with the policy in a mutually agreed way. This may be along the lines of certain specified devices will be permitted (and perhaps supported) by the IT department, providing they adhere to the security policy requirements.

- **Enforcement** - Responsibility is part of the shared commitment, and it has to be understood that there are consequences for misuse or careless behaviour. It is self-defeating if this removes a productivity gain, but without some level of penalty, or some benefit forfeit, users will soon fail to take security seriously.

There is a natural human tendency to try to keep things simple, and assume that everyone else has the same principles as oneself. While these are positive principles for life in general, there are reasons for an individual to be more careful and professional when valuable information or resources are placed in the employee's care by an employer. The ultimate aim of the security policy is to ensure that both organisation and individual take the matter sufficiently seriously.

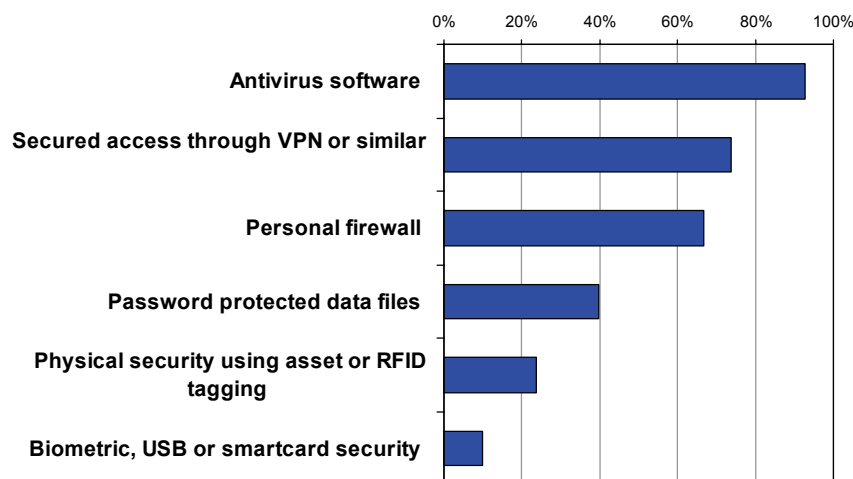
5. Supporting Policy with Technology

Whilst getting users to take seriously the security of any mobile technology they use, there are ways to supplement and support their professional behaviour with tools and basic procedures. Some of these will be inherent or common in existing IT systems; some will require further investment, and perhaps a level of bespoke integration. Before making this type of commitment, businesses would be wise to fully investigate what is already available from the suppliers of systems they plan to deploy, existing network management software suppliers, and the network operators or service providers used for connection.

It is important to remember that wireless and mobile devices can be easily brought into an office, either for good or malicious intent, and that not having an official deployment of a type of technology is no excuse for not safeguarding against it. For concerned businesses, there are several steps that can be taken. Monitoring wireless networks for rogue access points brought into the building, monitoring or fire-walling network traffic within sensitive areas of the corporate network, and controlling the points of access to removable data devices – memory cards, USB sticks, portable hard drives or even mobile handset synchronisation cradles - are all procedures which help. Most businesses already employ a wide range of security technology in particular for laptop users as these needs are well understood (Figure 8).

Figure 8

What security measures are currently in place for Laptops?



From 'Mobile Devices and Users' – Summer 2005

The best approach is to take a positive and proactive stance, even with no official deployment, to monitor, investigate and act. With this in mind there are a number of basic measures that most organisations should be able to take:

- **Passwords and PINs** – The simplest level of protection for any device or service is to apply a secret code for access. There are ways to break passwords with intelligent guessing or brute force - trying all combinations – and these can be defended by locking the account after a limited number of incorrect attempts. A suitable support route will allow legitimate users to find their way back. Passwords can be difficult to remember, but noting them down somewhere is very risky, so organisations should guide their employees in good ways to create memorable, but difficult to guess passwords. PINs offer less protection, but as a minimum should always be employed and changed from their out-of-the-box default setting.
- **Backup.** Loss of data through theft or loss of a device is a major concern that can be offset by an automated backup facility. If offered, this is an excellent service to acquire from an operator or service provider. Where the data volumes are large, some systems support an intelligent approach to detect and only transmit differences in the data, i.e. an incremental backup. For laptop users this is likely to be part of an enterprise wide backup capability.
- **Synchronisation.** Taking the backup concept a stage further and all relevant data can be synchronised in either direction between a central server and the mobile device. This ensures all devices are all in step with the same information, and that any data collected by one, can be automatically copied to the server. Full synchronisation also makes device failure easier to rectify, as a replacement can be simply reloaded with the synchronised contents of a faulty device.
- **Mobile antivirus protection** – For any laptop platform, this should be taken as read due to the enormous range of potential threats, but the argument for antivirus protection for mobile phones and networked PDAs is less clear cut. However devices based on the major mobile operating systems– Microsoft, RIM, Symbian, Palm, Linux – are becoming more sophisticated, and the threat from some form of malware inevitable. Even if risks are considered theoretical on some platforms, when tools are available to protect the platform from abuse, they should be considered for deployment. Mobile operators are already taking

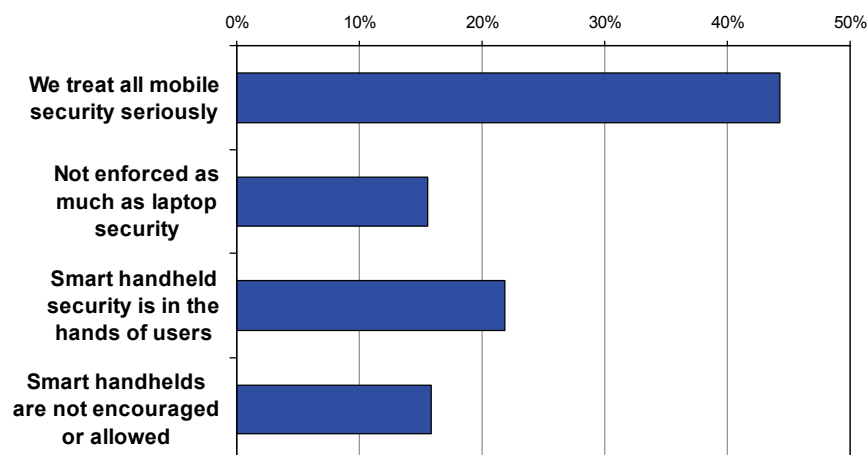
this threat seriously, by detecting the spurious communications from known rogue applications, but careless users can still undermine these efforts as mobile malware can exploit off network methods – memory cards, Bluetooth – to move from device to device.

- **Patch management** – Complex mobile devices, from laptops to smart handheld phones and PDAs run sophisticated software systems. No software is error-free, and the more complex, the more need for timely updates for bugs to be fixed and vulnerabilities detected and closed. This requires ongoing changes and patches to be applied to both underlying operating systems and applications to ensure that they are less likely to be compromised. Patch and upgrade management should be regarded as a security protection mechanism, not simply a logistical support activity. There are number of solutions for addressing the broader platform end point security needs ensuring patches, antivirus definitions and applications are up to date whenever the end point device comes back onto the network, or quarantining it if it cannot be fixed.
- **Lock and wipe** – Once a device is either lost or stolen, the most effective means of safeguarding as much as possible is to prevent the device being used and remove all data from it. This requires a network connection, and prompt action by the user to ensure success. The more this type of protection becomes commonplace, the less likely it is that devices will be stolen. The sharing of stolen mobile phone information between operators has already met with some success in this regard. User carelessness is still something to try to minimise, but at least locking the device from further use and wiping any valuable data offers a significant degree of protection.
- **Basic physical security** – A protective case not only safeguards against knocks and drops, but also reminds the user they have something valuable to carry. The more this fits with their personal requirements – light, unobtrusive, practical – the more likely they are to value the contents. For laptops, further physical security such as lockdown points and cable locks may seem useful, but if they interfere too much with user mobility they are less likely to be used, and just become an ignored, cumbersome burden.

Most of these basic measures are routinely employed by organisations deploying laptops, but frequently smart handheld devices are not as well secured (Figure 9). However these devices are more likely to be able to take advantage of synchronisation and lock and wipe technologies, due to the almost constant presence of a network connection, so with reasonable measures in place, organisations should be able to make these smaller devices more secure.

Figure 9

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



From 'Mobile Devices and Users' – Summer 2005

Beyond these basic measures, further steps can be taken, based on the level of risk, level of threat and sensitivity of the data being accessed. With greater security protection there often is greater restriction and inconvenience for the legitimate user, and so security must be balanced against the value being derived from the use of mobile services. These further steps might include:

- **Strong Authentication** - More secure access control than passwords or PINs can be obtained using strong authentication, such as a physical token to generate or store pass codes or otherwise grant access through their use, for example smart cards and secure token generators. Although harder to use on small devices, such as phones, where the device carries its own internal authentication token in the form of a SIM, strong user authentication gives more reliable security than a memorised password. When used in conjunction with single sign-on service, the additional complexity of using the token is offset by the simplifying of access across multiple devices or services.

- **Biometrics** – Using a unique token that is part of the user – retina scan, shape of a body part, but most often fingerprint – can provide a high degree of security that is relatively convenient to use as the ‘key’ is always with the user. In practice, this may mean a more limited set of devices can be deployed, and if they are prone to error, dust or dirty conditions of use, they are unlikely to be sufficiently robust to pacify user impatience. Again, if the risk demands, it may be worthy of consideration.
- **Active physical Security** – Physical security does not have to rely on pro-active user action. Tagging devices with radio frequency identity (RFID) tags, or for larger items Global Positioning System (GPS) locators can allow them to be tracked and traced through an environment, and will indicate if they are outside their permitted zone. Laptops and some larger handheld devices can be fitted with tamperproof trembler alarms which detect movement and require the user to enter a code to stop an ear-piercing alarm from sounding.
- **Encryption** - If data carried on a mobile device is really sensitive and the device supports encryption, then why not use it? Some users may find that the process is more tedious, so it’s rarely productive to apply encryption to everything. Base it on risk – either of stored data, data in transit, or both.
- **Destruction not deletion** – Devices taken out of service often will have data deleted from them and even disks reformatted, but this does not generally remove all the data from forensic investigation. Every block of data must be overwritten, or the storage device physically destroyed to ensure the information is really lost. This often only becomes necessary at the decommissioning stage, but is often forgotten, and is an important point of data vulnerability.
- **Firewall connection points** – Some devices that are mobile and wirelessly connected will also spend some time directly connected to the corporate network through a synchronisation cable or cradle to a desktop computer. This is another vulnerable point, and firewall and antivirus protection for that desktop will defend the rest of the network from spreading infection if the mobile device has been compromised in some way. Mobile devices can easily carry malware even if they are not infected by it.
- **Trusting mobile code** – Email attachments, downloaded programs and executables taken off a memory stick can all be suspect. Good practice is to warn users to be suspicious of email attachments from unknown sources, especially executable programs, but this should be well known as it is just the same on desktop computers. Software picked up dynamically as downloads or from memory cards can be signed with a public key. Using this approach for internally created and third-party mobile applications increases the level of trust in the content. Being out of the office, in a rush to meet a deadline, or dealing with something hurriedly on a small screen is no excuse for lack of care.
- **Display protection** – The improving quality of displays with increased clarity and brightness from wider angles opens up the opportunity for ‘shoulder surfing’, where the attacker looks over the victim’s shoulder and gleans secret data, passwords or other information. Screen filters are available to narrow down the field of view, so that for example only the user of a laptop can see the screen. Arguably a similar problem exists for those users who bellow into their mobile phones, and there have been solutions to close off the area around the microphone, but a more practical approach would be to engender sensible mobile phone etiquette amongst callers in public places.

6. Broader good business practices

As well as looking closely at the security of the mobile devices, the users and the connections they use, there are other broader good business practices that have an impact on mobile security. This can be the case even for those that are designed to meet other business needs, sometimes outside the remit of the IT function. This is another reason for keeping the overall responsibility for security outside of any one functional department, and placing it at a more senior level of responsibility.

One basic process is asset management. While some mobile devices themselves are of low value, and cheap and easy to replace, the access rights they grant and the content they contain may be far more valuable. Asset management should start with the receipt of goods, and end when the asset is decommissioned. Upon receipt, serial numbers should be recorded, and for mobile phones this should also include IMEI numbers so that assets lost can be quickly identified and locked by the network provider.

At the end of an asset's working life, decommissioning should take into account the organisation's wider policies. Will it be recycled, reused or resold? If so has all data been wiped, has all owned and licensed software been removed? This is not only good security practice, but for many organisations could form part of their requirements for complying with government procedures or external directives.

All companies in Europe now have to take greater notice of the EU Waste Electrical and Electronic Equipment directives. While these have their greatest effect on suppliers, some of this will be passed onto the purchasers of IT and telecommunications equipment. A little extra effort in this area is not only good for the environment, but is also a positive and pro-active way to approach asset control.

Of potentially farther reaching impact are the EU directives on data protection and restrictions on software licenses. Businesses have a responsibility to safeguard third party personal information they process or control, and have to show they have procedures to manage this information. There have been a number of high profile stories in the media where large companies have disposed of computing equipment, only for it to be found to be containing personal and sensitive business information. Whether the disposal is part of an official redeployment process, or an individual selling on an unwanted business asset is irrelevant, care should always be taken to ensure the asset is clean of data and that software products that are licensed specifically to the original owner are not illegally transferred.

Some devices have ways to truly delete the data stored on them, but this varies from device to device and may require probing questions of the supplier. Where a suitable tool or command exists it should be used to wipe all data before passing to another user or re-deploying elsewhere. If critical information may be at risk, and no reliable soft wipe method can be used, the ultimate fail-safe is physical destruction. It may seem extreme, but in the last resort, it might be the correct approach.

It is important to identify who is responsible for looking after an asset. When a mobile phone, laptop or other corporate supplied mobile device is issued to an employee, there should be a formal process in place. This is another control point for ensuring that the employee has understood their responsibilities to look after the mobile device, its data and resources it uses. It can also provide a check for both employee and employer to see that default security settings are appropriate, and that the employee assigns an initial password or PIN if that is company policy. A similar process should be undertaken when the employee returns the device, and the safe return is acknowledged. It should be possible at any moment in time to report which items are in the care of which employees, and so loss, theft and replacements also need to be noted.

As employees join the organisation or switch roles - moves, adds and changes – this further complicates the administration of assets. It is clear that when someone leaves employment they should no longer have access to the corporate network, but not always noticed that a promotion or change of role should lead to a change of access rights or capabilities. While these may not be abused deliberately by the employee concerned, it could provide a loophole for unscrupulous use in the future. At the very least, it does not reflect the level of control that should be enforced.

7. Conclusions

Security in the IT and communications world is often seen as a technical discipline, when in reality it is about the organisation's attitude to risk. It is one aspect of the running of any organisation that may affect its ability to function, and should be treated seriously as part of the overall resilience of the business to internal and external events.

Mobile technologies and communications have transformed the way businesses and individuals interact, and extended the use of IT assets and resources from the constraints of the desktop to be right next to the user where they can deliver the most benefit. There is no doubt that taking access to corporate IT systems, and sophisticated communications tools outside the physical confines of the office exposes the organisation, and in some cases the individual employee to greater risk, but this has to be offset by the value returned. These risks can be managed through the application of a sound security policy that fits the business needs, and is supported by effective tools and procedures.

Even companies with well thought out policies and well implemented solutions need to generate the right attitude and approach to security among their users. A pragmatic approach to security has to take into account how dependant the organisation is on the individuals who work for it, and the attitude they take. Involving them from the outset and taking into account the personal impact of mobile technologies and communications will encourage buy-in and greater commitment to safeguarding the resources of their employer. It helps if personal responsibility for security is seen as part of the broader issue of the etiquette and management of remote and mobile working, where employer and employee challenges overlap.

All of these measures are aimed at managing and containing risk, but organisations should always prepare for the worst case scenarios. Ultimately business risk is a commercial decision, and may need to be offset further by financial measures, including insurance. This is only likely to provide compensation for the loss of material goods, for example the laptops and phones, and not the intellectual property, goodwill and reputation that a security lapse may damage. These risks must also be managed.

However, organisations of all sizes and types derive many benefits from instant mobile access to communications and individual employees have gained greater flexibility in both their work and home life. It is important that these benefits are not undermined by an overly restrictive attitude to security. The best way to deal with the risks is to minimise them by taking positive steps to manage the mobile security challenges. That way organisations and individuals can continue to be safe and secure and take full advantage of mobile technology.

APPENDIX A Threats to Mobile Users and Devices

- **Malware.** The overall term for any sort of malicious software, not specific to mobile devices, but applicable to any type of software that has malicious or mischievous intent.
- **Virus.** The most notorious form of malware as they have been the most prominent for end users. A virus is generally attached to another program and has the ability to replicate but is typically spread by user action, such as clicking on an executable program. Some virus are just intended to propagate, but more often their intention is to deliver a 'payload', which is the damaging part.
- **Worm.** These are similar to viruses, but are self-contained programs designed to replicate and propagate onto other systems as well as performing some function on their current host. The self-replicating nature can lead to network and system overload
- **Trojan/Trojan Horse.** These take the form of malicious software hidden inside another application, interesting software, or under another name that the user might trust. When run they appear to operate as the user expects, but are performing their hidden or malicious purpose in the background. Most often spread directly by users over email or on storage media like memory cards. Does not replicate
- **Spyware.** A generic term for any software that intercepts information or takes partial control to monitor in secret. Often appears as a result of visiting a web site, and the spyware takes an active interest in user actions or might simply deliver a pop-up window.
- **Denial of Service.** An attack that attempts to overload a system, network or resource. While not actually damaging to the machine or device under attack, it does prevent or hinder its legitimate use.
- **Eavesdropping.** There are many ways to spy or listen in on conversations or spy on information on computer screens that do not involve technology, but an inquisitive eye or ear, and a careless user. This can be especially a concern with mobile phones and increasingly smarter mobile devices.
- **Social Engineering.** This is the attempt to trick someone to reveal more information than they should, and more often relies on people's helpful attitude and low likelihood of checking credentials of what seems like an innocent request. It might start with questions for what seems like innocuous information, but the threat comes from piecing information together from a number of sources.
- **Phishing.** A form of social engineering type attack where the attacker pretends to be an official or recognised body, and asks the victim for personal or valuable information such as bank account details. Relies on the victim not checking for suitable credentials.
- **SPAM.** An unwanted and un-requested message or transmission. The name originates from the British TV program Monty Python about a café in which "spam" came with every menu offering. This meat dish, Spiced Pork with hAM, is not widely regarded as an interesting or tempting product, but is valued by a small minority – much the same could be said of electronic spam.
- **SPIT.** Spam over Internet Telephony. Unwanted and un-requested voice calls. Whilst cold-calling is widely used, it can be controlled to some extent by traditional national phone companies. This becomes a far harder challenge as voice telephony is moved over generic IP networks.
- **VOMIT.** Voice over Misconfigured IP Telephony. An unwelcome mnemonic, but transmitting voice over IP networks does increase the scope for configuration errors
- **Bluejacking.** This is sending messages to Bluetooth devices in range. It has been viewed as little more than fun in social situations, but could be used to encourage a victim to expose more information.
- **Bluetracking.** It is possible to track someone's movements by identifying their Bluetooth device. Each device has a unique address, so sensors can detect where a particular Bluetooth device pops up and record a person's movement. This does require specialised equipment.
- **Bluesnarfing.** Some mobile devices, particularly certain phones are vulnerable to direct attack using a Bluetooth connection to extract information stored on the device. Hackers can obtain phonebooks, calendars and stored SMS messages.
- **Bluesniper.** This is a working prototype device made from a rifle stock with a scope and Yagi high gain antenna attached. This allows Bluetooth signals to be precisely picked up over a far longer range than normal, and the signal then fed into a Bluetooth enabled /PDA or laptop.
- **Bluebugging.** This involves sending requests to a Bluetooth device to use it as a listening device. It does require software on the phone to respond, but in combination with a suitable Trojan, this is a reasonable concern.

About Orange Business Services

Orange Business Services represents the business communications solutions and services provided by the France Telecom Group as of June 1st, 2006. They were previously sold under the France Telecom, Orange, Equant, Etrali, Almerys, EGT, Expertel Consulting, France Telecom Intelmatique, SETIB and Solicia brands.

The offers include converged voice, data and mobile services as well as IT expertise and managed services, all designed to transform business processes and improve productivity. Orange Business Services is present in 166 countries and territories and serves customers in 220.

About Orange

Orange is a key brand of the France Telecom Group, one of the world's leading telecommunications operators with 149 million customers on five continents.

In June, 2006, as part of the France Telecom Group integrated operator strategy (NExT programme) to deliver simple, convergent products, Orange became the single brand for mobile, broadband and multiplay offers in France, the United Kingdom and The Netherlands, strengthening Orange's position as the number two mobile and internet services brand in Europe. In addition, Orange Business Services became the new banner for business communications solutions and services. Orange Business Services is present in 166 countries and territories and serves customers in 220.

The France Telecom Group has 23 mobile and nine internet operations across the world. At July 27, 2006, the group had 88.6 million mobile customers, and 11.9 million internet customers.

Orange and any other Orange product or service names included in this material are trade marks of Orange Personal Communications Services Limited. Further information can be found on the Orange website at www.orange-business.com

**Business
Services**



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.