



## Carrying the can

---

*The corporate-liable versus employee-liable balancing act for mobile*

**June 2011**

There is an increasing trend among employees to want to use their personal choice of mobile device in the fulfilment of their work commitments. While this appears to bring many benefits for the employee to select their preferred device or devices and, on the face of it, reduces upfront costs for their employer, it does introduce significant on-going costs and risks for the organisation. However, with many appealing mobile consumer devices being offered, the trend is likely to increase, so organisations need to work out suitable strategies and policies to manage this complex and hybrid situation in the best interests of both themselves and their employees.

Rob Bamforth  
Quocirca Ltd  
Tel : +44 7802 175796  
Email: [Rob.Bamforth@Quocirca.com](mailto:Rob.Bamforth@Quocirca.com)

Clive Longbottom  
Quocirca Ltd  
Tel: +44 118 9483360  
Email: [Clive.Longbottom@Quocirca.com](mailto:Clive.Longbottom@Quocirca.com)

# Carrying the can

## *The corporate-liable versus employee-liable balancing act for mobile*

*Consumer technologies and attitudes are rapidly entering the workplace. Organisations must develop a workable and efficient strategy for dealing with three major issues surrounding employee use of smart mobile devices – device ‘consumerisation’, connection contracts and payment, and the secure management of content or applications. The balance between what is owned and provided by the business versus what is introduced by the employee (e.g. BYOD – bring your own device) needs careful consideration. Overall, this is often referred to as evaluating whether mobile deployments are ‘corporate-liable’ or ‘employee-liable’, which this report will explore further, along with the implications for the organisation.*

### **Mobile working is no longer a minority activity**

Faster and ubiquitous connections, combined with smarter small devices, have not only made it possible for work involving IT access to be conducted away from the desk but also, with a new generation of touch screen tablet devices, it is almost mandatory. These technologies have become ingrained in consumer behaviour through the widespread acceptance and use of the internet and social media. Organisations are no longer dealing with a handful of individual mobile ‘road warriors’, but a whole army of workers with different expectations and needs.

### **Touch screen tablets are popular for home and work**

Whether this is an alternative to a laptop or simply an extra mobile device does not matter, tablets bring an informal approach to accessing content and communicating that could add to security risks. The fact that many individuals will already have one for personal use will mean that this class of device is a very likely contender for a ‘bring your own’ device. On the flip side, corporate-issue tablets are very likely to have personal use, so either way it will be important to understand how they fit in to the corporate mobile strategy.

### **Consumerisation of IT means users have strong opinions and want to choose**

Technology was once more advanced in the workplace than at home but, for many workers, this is no longer the case. Not only has consumer IT become pervasive, it is simpler to use and appealing. Individuals buy consumer technology to match their personal taste, style, image and aspirations, and would like their work options to match their consumer preferences. One group of employees in particular, senior executives, sometimes use (or abuse) their position to compel IT departments to allow these personal choices to be brought into the work domain.

### **Savings in device purchasing mask contract issues and hidden costs**

Who buys the device might bring potential upfront savings, but there are unexpected consequences for higher costs elsewhere. Organisations need to be clear that they understand what these are – such as what network tariffs are being used, what is the impact on software and support, are some people unable to function properly because their choices are incompatible in some way (e.g. with their role, or with other users or other technologies used in the business)?

### **Consumer attitudes to mobile apps and content introduce risks**

There is no point trying to turn a blind eye or ignoring the inevitable. Most organisations are probably unaware of the number of consumer devices that employees use for work purposes or what personal use they make of corporate network resources. While the organisation might not want to, for example, block access to social networking or frisk employees for memory sticks, it does need to understand what is happening, assess the exposure to risk, and put in place suitable policies and protection.

### **The organisation has to monitor and keep a level of control either way**

Whether mobile devices are company owned or employee owned, if they are used on the organisation’s network to access the organisation’s assets, the organisation has a responsibility to measure, check and provide safeguards. This is not only to secure data, but also to secure the best value for the lowest overall cost to the organisation. Done well, this will not constrain the employee but will introduce benefits for them.

## **Conclusions**

The reality is that this is no longer an issue to avoid. Employees will have their own mobile devices and many will, at times, want to use them for work purposes, even if only occasionally. This consumerisation of device is not the same as dealing with network contracts or billing, but is often conflating them and together has an impact. Dealing with the issues this raises is something all organisations should take a pro-active stance on now if they want to avoid costs and security risks down the line.



# Introduction - the mobile device dilemma

## Time to pack up the desk

Predicting the demise of the desk has been a bit like predicting the paperless office. While great in theory, there are many constraints, often personal and social rather than technical, which makes the reality somewhat more complex to achieve. However, the comfort and attachment to wood, aluminium and generally cheap veneer is wearing thin for a number of reasons, some driven by the organisation but, perhaps more importantly, many others driven by the individual. Mobile is becoming a default and accepted way of working.

Everyone has not suddenly adopted the fully nomadic working style of a 'road warrior', sales rep or field service engineer, but while most business activities are dependent on access to IT, this is no longer an activity that requires participants to sit at a dedicated place to use their access device. Mobile working is moving about the office, just as much as driving down motorways, sitting in airport lounges or logging in from a study at home.

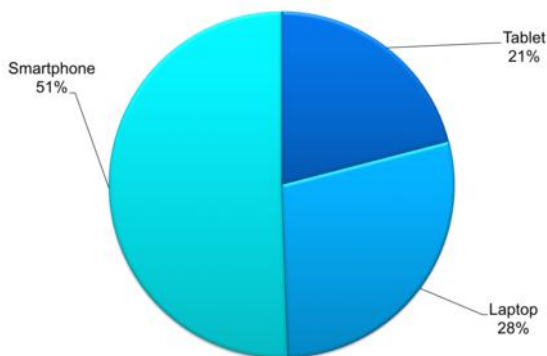
The advantages for the business have been trumpeted for some time; the potential to downsize real estate and lower costs of facilities or office space and boost productivity, effectiveness and responsiveness of employees. The former can be implemented with flexible office and hot-desking programs and renegotiation of rents or the sale of assets, but the latter depends heavily on the commitment of the individual employee.

## Consumerisation of mobile devices

Whereas once this sort of commitment was hard to stimulate with corporate issue laptops and mobile phones best suited to road warriors and yuppies, the pervasive consumer adoption of mobile phones, the internet, social media and new shiny devices have made mobile technology desirable. On the face of it, this might make mobile working easier to do, but it introduces many complexities due to the increasing numbers of mobile devices being used by employees as consumers and a huge diversity of choices of devices, with brand and style appeal.

Figure 1

**If you had only one mobile device, what would it be?<sup>1</sup>**



The laptop and mobile phone are rapidly being usurped by the smartphone and now the 'new' tablet form factor - connected devices with the convenience of mobile phones, but the power of laptops and simpler usability than traditional desktop computers. These converging mobile devices are enabling users to contemplate carrying only one device, with interesting results.

Part of the swing towards smartphones and tablets is due to the significant consumer success of Apple and now the Android platforms. These devices capitalise on ease of use, internet connection and the availability of a huge number of cheap or free applications. They deliver a social and media connection on the move

which is so appealing that most do not want to lose this lifestyle accessory while at work. This leads to a significant increase in the amount of mobile data usage.



## Organisational control

Herein lies the problem. Consumers have become ardent fans of the technologies that might make them more productive as employees, but they are unlikely to want to have less capable devices for their work, be restricted as to which services they can access, or be keen to carry multiple devices for home and work. They like the opportunity of personal preference and individual choice. However, the organisation needs to retain control to ensure the security of its IT assets, protect its liabilities and manage costs.

On the face of it, adopting an individual-liable approach could be of significant value to the enterprise, by simplifying or removing a number of difficult issues. Indeed, if this were just about the purchase and use of standalone tools, passing the responsibility to the individual would be very worthwhile. The complexity for the enterprise comes from the fact that it is not simply about the device, but a number of interlinked factors:
















- **Hardware** – not only the cost of buying the devices, but also peripherals from earphones and Bluetooth headsets to docking stations and chargers. Most of these are very personal and will depend on the individual, so providing a ‘standard issue’ set that would work for all would be expensive. Over an employee’s tenure there may be upgrades, replacements and companion devices required.
- **Applications** – even the smallest mobile handsets have significant compute power and storage, and can download anything from ringtones to full blown applications. Most employees, whether using a company-issued or personally acquired device will want some ‘non-corporate’ applications. These might be unofficial, but still useful for their day to day work, such as for travel – train timetables, airline departure apps, currency conversion – or note recording, reminders, shipment trackers, etc.
- **Networks** – no longer simply business phone calls, but a mix of personal and work activities that eat into data, minute and text tariff pools. SIM swapping from corporate feature phones to employee-owned smartphones is becoming a major issue now that all SIMs are data-capable and data usage outside of a proper tariff will incur large pay-as-you-go charges. What should be permitted, banned or paid for by the employee? While tariffs have been slowly falling over time, usage is rising and, with a varied mix of applications on a myriad of devices, in an unpredictable way. Measuring worth and cost of network use is now very complex.
- **Usage** – not only are network resources consumed in a complex way, but so too is time. Mobile devices are often justified based on productivity gains and responsiveness, but how much more time and efficiency do individuals lose by not paying full attention due to legitimate interruptions, alerts or entertaining distractions from their always on, always online mobile companions?



# Impact of employee choice on cost

The shift towards an employee-liable approach is often justified along the following lines. Employees already have their own preferences of mobile devices as consumers, and allowing them to exercise that choice for work will create less friction and make it easier to recruit suitable employees. It will also then save the organisation from having the upfront capital cost for more expensive pieces of hardware.

However, it is a mistake to confuse employee-liability with consumer choice of mobile hardware – there are other issues to consider, and these begin to highlight where some of the broader impact will be. Organisations need to consider how far they want to be along the scale of handing over mobile liabilities to individuals. With cellular-connected mobile devices, there is a specific area of cost that must be borne whoever provides the hardware – the mobile contract. This has considerable ramifications for both individual and organisation. The contracts, tariffs and who pays what for business and personal usage are major factors in determining the actual lifetime costs of corporate- or employee-liable approaches.

	Contract	Device	Payment
<b>CORPORATE</b> Complete corporate liability			
<b>CHOICE</b> Corporate liability, with consumerisation			
<b>CHARGED</b> Corporate liability with end user payment			
<b>CONSEQUENCES</b> Corporate liability with consumerisation and payment			
<b>PERSONAL</b> Complete individual liability			

Does responsibility lie, with the organisation



or the individual?






There are different cost impacts on the organisation depending on if the individual is responsible for contract, device and payment.



**Contracts**

These are generally constructed to keep costs down and reduce complexity for the organisation, so, on the face of it, handing ownership and responsibility to the employee seems like a good idea. However this is a massive loss in terms of ‘economies of scale’ and, while individual contracts will be lucrative for the carriers, they will generally be more expensive for both the individual and organisation.

Contract costs	Individual responsible	Impact
Device upgrades	Existing contract termination – most users will have the latest device because they have been offered it as part of the deal for extending their existing private contract. If that device is to become a ‘bring your own’ into work they will need to terminate the private contract, but who will pay?	£
Helpdesk support	Normally needs to be put in place and available to all users, ideally on a 24x7 basis, but if the employee has their own contract, this will be with the service provider or up to the individual to manage, either online or with peers. This will impact mobile device effectiveness of employees.	£
Network tariffs	Volume discounts no longer apply. Mobile to mobile, mobile to landline, landline to mobile on-net rates are very competitive and normally around 1/3 <sup>rd</sup> of the cost of cross network calling. If users are allowed to have multi-network options this will increase both mobile and landline costs.	£
Network bonuses	The bonuses paid by the networks for the corporate contract are likely to be lost. These bonuses have been paid in a variety of ways, but are a value that could diminish very quickly and one that must be accounted for.	£
Data consumption	Data is purchased in ‘bundles’ but with no way of segregating business and personal data usage, so no mechanism to re-coup personal data consumption costs. Based on average personal call statistics of 28% of all calls, personal data usage could be far more significant.	£

What is the impact on the organisation – Negative  Neutral  Positive 

The key to reducing and controlling costs is accountability through the cost centre architecture all the way down to end users. With individuals taking contract responsibility and reclaiming through expenses all accountability is lost in a stack of paper, paid monthly with no easy method or extensive resource burden to validate claims, payments, usage and personal call deductions, let alone any way to validate network billing charges.

This approach now comes with far greater implications, with data becoming the norm on business connections and being supplied in ‘bundles’. Organisations cannot possibly expect users to be able to evaluate their data consumption and adjust the data bundle to best suit their usage profile. It would be naive for organisations to believe that this is the role of the network – this is their own in-house management issue and trying to push this out to the networks as their responsibility is not a business-like approach. It is the equivalent of sending a bank statement to a bank manager to check.

Most organisations that have signed/re-signed new contracts in the last 18 months may not be aware that voice connections are no longer limited to voice calls. Networks, by default, set up contracts so that all voice connections automatically include pay-as-you-go data. This is a management headache for organisations to control costs, and especially the usage of data, because of the risk of SIM swapping from a business-supplied phone into an employee-owned device. Users that SIM swap from a conventional voice-only connection device to a feature rich data-centric device find that data will work and do not question whether they should or should not be using it – they believe it’s the norm. Pay-as-you-go will prove a very expensive way of using data compared to an agreed and negotiated contract tariff.






**Devices**

Again, when mobile devices were simply phones, the desire for an employee to want their own particular type of device was only slight. Now a diversity of smartphones and tablets, strong consumer brands and a wholesale acceptance of technology in many people’s personal lives means that many employees will have strong opinions about what they do, and do not, like or want to be seen with.

This is where the much-discussed consumerisation of the enterprise appears to generate the most gain for the organisation; however, even here the initial capital cost savings can quickly be undermined. For many employees, there may be unexpected costs that previously were absorbed by the organisation.

Device costs	Individual responsible	Impact
Upfront cost	Should be borne by the employee, although a halfway house where employees are offered an allowance providing they choose a ‘suitable’ device might be used.	£
Device unlocking	Almost all handsets will need to be unlatched from their originating network. This costs between £10 and £30. There are cheaper ‘backstreet’ options but this inevitably renders warranties null and void.	£
Device Management – service support	Individually bought devices have consumer support models, with extended wait times for in-warranty replacements. This is the responsibility of the user who risks being ‘off-air’ while waiting, which may impact their ability to work.	£
Replacement costs	Operator subsidy over the contract lifetime is a major driver for adoption of the consumer mobile devices. Users seldom understand the real or replacement cost.	£
Valid procurement	Strict rules are necessary where the user buys their own device e.g. if using eBay or certain other channels the user could be buying a ‘grey’ import with no support and with completely different software to the norm for that country. Even buying from recognised dealers can cause issues with support timescales.	£
Mobile policy	With devices being brought in by individuals, mobile policies will need to be put in place and certainly beefed up. This is required even in organisations that do not routinely provide mobile devices for their employees, as employees will bring in personal devices in any event.	£
Software platforms	Standard builds and volume discounts keep the cost of providing a common software platform low, but not if the employees choose their own devices. Organisations will have to provide and pay for software e.g. malware protection even on employee-provided devices – platform diversity will increase licence costs.	£
Application availability	More workload in IT to ensure applications are available or that there are alternatives for the range of devices employees choose.	£
Data bolt-on	Where many corporate devices might have had voice-only tariffs, once employees provide their own devices into corporate fleets, data bolt-ons will be required to be added on to the contract. Over a large fleet of mobile employees this will have a considerable cost impact.	£

What is the impact on the organisation – Negative  Neutral  Positive 



**Payment**

Working out an acceptable accountability model so that individuals pay for personal use and the organisation pays for business use has been difficult enough to implement with voice calls, but becomes impossible with data consumption on smartphones and tablets. Where the organisation is responsible for payment, this will involve claims and expenses processing, which is a costly system to run, but without such controls employee abuse could be rife.

If the individual is responsible for making payments, it is most likely they will want to claim the business elements of their expenses back. This is fraught with difficulties because, while business and personal phone calls might be relatively easy to identify, they are difficult to verify by the organisation as the bill belongs to the individual. However since mobile data is rapidly becoming a significant element of mobile tariffs, especially while roaming, allocating this fairly or accurately between business and personal is pretty much impossible.

Payment costs	Individual responsible	Impact
Personal use	No longer needs to be monitored and recovered as a cost, but employees who are paying their own bills may be tempted to spend more time on personal activities when they should be working. When controlled by the organisation this can be monitored automatically, but otherwise will need well communicated and understood policies to ensure appropriate employee behaviours.	£
Carbon Friendly	Individual liability means INDIVIDUAL billing; some may be online, others on paper, but probably requiring printouts for reclaim, so not very carbon friendly.	£
Expense Reclaim	The cost of processing expense claims is not free and one that many organisations overlook or fail to take into account. The average cost associated with processing is roughly £40–£50 per claim and can quickly mount up. A number of employees are likely to be claiming expenses already, so adding a line seems trivial but many users will not be claiming expenses on a monthly basis so this may generate considerable extra work if processing 100/1000's of mobile invoices.	£
Policing & Compliance	With billing data sent direct to users there is very little organisations can do to analyse billing data without the consent of users – individual billing makes data personal even if there is ultimate corporate liability.	£
Monitoring & validation	Monitoring and validation is non-existent when it comes to expense-paid mobile bills. Mobile expenditure gets lost and it is almost impossible to provide accurate management information. After all – who is going to go through 1000's of paper bills to check if a user has allocated personal calls correctly or if at all?	£

What is the impact on the organisation – Negative £ Neutral £ Positive £



# Impact of employee choice on risk

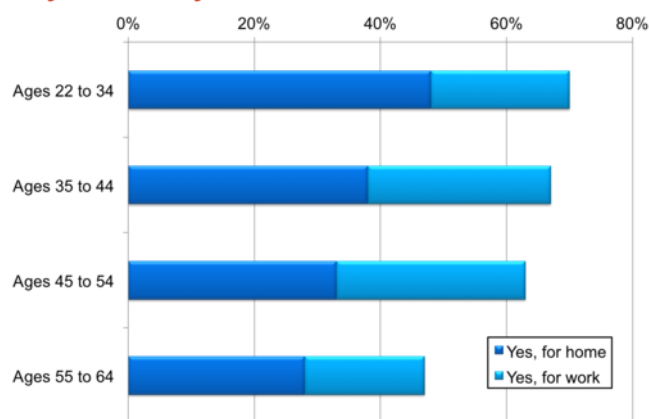
From the employee's perspective, taking the matter of mobile devices into their own hands makes sense. Consumer products have made IT and communications technology accessible, simple to use and with a relatively low upfront cost. Improvements in quality and design means individuals are more confident that the technology is unlikely to break down or, if it does, they can ask a friend, look online for help, or, as a last resort, read a manual or contact a supplier support centre.

The 'razor and blades' commercial models prevalent with most aspects of consumer technology encourage initial purchase and stimulate on-going usage. So connection costs and software and media purchases are spread over time and individually look insignificant, although the build up over time with ever-increasing usage might be considerably more significant.

Beyond racking up excessive costs, the risks for the individual for their own purchases are loss of hardware (often mitigated with insurance), loss of media or application content (generally mitigated with synchronisation to another device or a 'cloud' service) or infection by some form of malware. For most, these are minor concerns compared to the benefits of using the technology.

**Figure 2**

## Do you currently have a tablet device?!



With these consumer expectations in mind, it should be no surprise that employees would then also expect to use their consumer devices for work purposes.

This is particularly prevalent among younger members of the workforce, many of whom have already wholeheartedly adopted new mobile technologies for personal use – the latest generation of touch screen tablets being a case in point. Those who have adopted tablets for personal use will increasingly be using it for work purposes – indeed will expect an enhanced experience through such devices.

Interestingly, a larger percentage of older employees already have tablet devices for work purposes and, as they will undoubtedly discover personal uses for these devices, there will be a growing crossover between workplace needs and personal needs right across the age spectrum.

While this crossover might seem reasonable for the employee, it does open up significant levels of risk for the organisation, and these increase if the organisation does not own or control the underlying device.

Many of these risks are exacerbated by the double-edged popularity of consumer applications and social media, which opens up a multitude of opportunities for employees to waste time and mobile network capacity. Encouraging employees to work while mobile with tools and network access on the assumption that it will make them more productive might be a forlorn hope unless suitable on-going checks or measurable outcomes are in place.

There are many disadvantages to the organisation if employees choose such a wide variety of options that compatibility issues creep in. Not only will this affect who has access to what facilities, it will make it harder to provide technical support and harder to ensure data integrity and that adequate measures are in place for backup.



Risk	Individual responsible	Impact
Device acceptance	Individual more likely to look after and take better care of their own device, keeping its corporate content and access safer	£
Inappropriate content	Organisations can do little to monitor or control the content of employees' own devices and, if they do, this can lead to employee concerns about privacy	£
Tax implications	Need to be understood and correctly monitored with respect to personal calls and potential changes in the approach to benefits in kind.	£
Security management	Organisation needs to put watertight policies and education in place to ensure individuals suitably equip their devices, or have constrained access to corporate resources.	£
Security support	Consideration needs to be made for the cost of supporting security software, platforms and servers, whether supported internally or externally – this will cost.	£
Data integrity & backup	Requires individual support and may be more ad hoc than organisation would prefer.	£
Technical support	Organisation may encounter unknown and unexpected issues that individuals are unlikely to resolve themselves or directly with providers.	£
Breadth of support	Supporting different operating systems across an unknown range of mobile platforms swells the level of knowledge required or forces users to do it themselves.	£
Incompatibility	Despite initiatives such as Java, and the growing market share of platforms such as Android, the lack of a common mobile application platform means that, with open choices, there will be some incompatibility.	£
Cohesion	Some employees, e.g. senior executives, may object to having to self-support, and still expect the IT department to help them, meaning IT spends more time on ad hoc queries or fire-fighting.	£

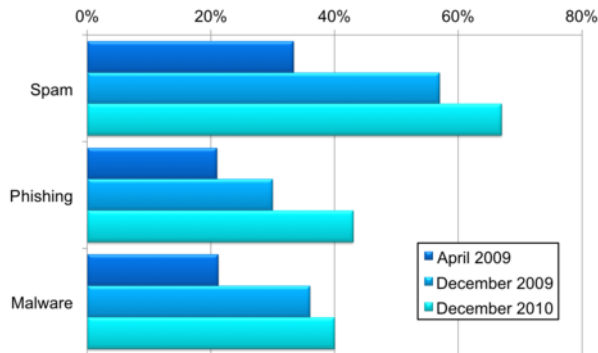
What is the impact on the organisation – Negative £ Neutral £ Positive £

Security is a significant issue. While many organisations are investing to make use of social networking as a positive tool for business, almost 60% of organisations surveyed in Sophos' 2011 security report thought that an employee's behaviour on social networking sites could endanger security at their organisation.

The growth of malware in social networks is a particular cause for concern, especially if employee social media on devices used for work purposes is ignored or poorly monitored.



**Figure 3**  
**Those reporting spam, phishing attempts or receiving malware on social networks<sup>2</sup>**



Security is always a problem with mobile devices used for business purposes, with the risk of the loss of data as well as the hardware itself, from theft or loss of the device. This might be mitigated somewhat with BYOD for business use, as employees are more likely to take care of their own possessions than those they might feel are substandard and have been imposed on them.

However this is unlikely to be sufficient for the organisation, many of which will consider it to be necessary to protect corporate assets on employee owned devices, through installing security agent software, a protected sandbox, virtualisation or even whole device encryption. How deep the organisation

reaches into an individual’s own device will have implications, especially in the event of termination of employment. There is also the risk that too heavy handed or constraining an approach will choke off the very benefits that organisations were hoping their employees would gain from being able to choose consumer mobile devices.

While the positive side of the employee-liable approach is that employees might be more careful with their own hardware, their use of social networking on devices used for work as well as personal activities might expose the organisation to malware risk and data leakage. This needs to be adequately addressed by the organisation if BYOD is to be acceptable.

There are further issues with access to content that affect IT policies. Unless organisations ensure all mobile web traffic is routed through internal access points then users with mobile web devices using public network access points will be able to visit sites that would normally be restricted on internal access points. If a mobile user can access these sites and an internal user cannot - how should IT policy deal with this, especially as it cannot be monitored? If both sets of users know this, there is a risk of claims of ‘discrimination’. This then raises a further HR issue if users are accessing sites on company devices that are considered inappropriate.



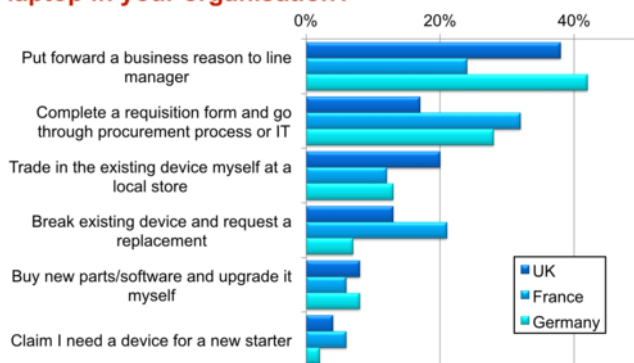
# Mobile strategy and policies

Many organisations seem unable to know what to do in the face of the relentless consumer pressure for device choice, with consequent fragmentation of network tariffs and potential risk to corporate assets and for abuse of resources and time. They should start by defining a mobile strategy - something most organisations fail to do, hence why many mobile deployments have been ad hoc - and consequent policies.

These have to encompass the organisation's attitude to risk and security, cost control and monitoring and broader reasons or value expected from the adoption and use of mobile devices. This will then determine the approach to where it is necessary to insist on tight control and where it is acceptable for employees to do things for themselves.

Figure 4

## What is the quickest way to get a new phone or laptop in your organisation?<sup>3</sup>



Not all employees will want this freedom, even if offered, and will welcome the clearly defined parameters that allow them to separate work and personal activities. They might have to carry their own personal mobile device as well as one for work, but the clarity of physical separation offers benefits for both employer and employee.

Mobile strategy and policies need to be established in collaboration between line of business management, individuals and IT or resource management, and not some dictat from an embattled IT manager, penny pinching finance director or overly prescriptive individual in HR. Ingenious or disgruntled employees will always find

ways round what they perceive as inappropriate constraints, even if it means damaging corporate assets.

Some senior executives go and buy devices themselves and will then approach IT demanding they make it work, so almost all organisations will have to consider the implications of allowing at least some employees to bring their own devices. The challenge for the organisation is to ensure that any short-term cost savings or apparent values gained are not overwhelmed by other hidden costs or exposure to risks that prove expensive in the longer term.



# Conclusions

---

The increased acceptance and use of advanced communications technology in everyday life means that individuals as consumers have access to more advanced technology than they may do at work. They may therefore feel that their employer is not providing them with the most effective tools to match:

- **work needs** - to carry out their role as effectively as possible
- **social needs** - status, prestige, being part of the gang, etc.
- **personal needs** - applications or services they need or want to use daily

With regular mobile phones, the main issues surround keeping a tab on the mix of business and personal use and deciding who pays the bills. With smartphones and tablets the issues expand to application usage – will they introduce security issues, will personal use escalate, how much extra support will employees need? Whether these smart mobile devices are provided by the organisation or the individual makes a difference, but, critically, so does the ownership and management of the contract. The reality is that all organisations will have to find a way to deal with employees bringing in their own devices, so it is best to incorporate this into the enterprise mobile strategy.

Organisations need to act fast to put policies in place to retain an element of control. This is already an issue and there will be a confusing mix of both corporate- and employee-liable devices. There is no single, simple solution and users will need to be profiled, based on the needs of their role, so different ground rules can be established for differing business needs.

The organisation has to decide where consistency is important or vital. This may involve some commonality of devices, but the main aim should be to determine common commercial and operational platforms independent of the actual device. The commercial platform has to take into account all elements of the contracts used for connectivity and what elements employees must pay for. The operational platform should provide the levels and types of access, security and malware protection required and whether the individual or the company provides the device. Where an employee's choice of device does not fit with what the organisation needs to deliver in terms of a suitable platform for work, the employee needs to be made fully aware of the limitations of their choice and the impact it will make on their work.

There are certain 'must have' devices that are going to have broad employee appeal, and organisations would do well to recognise this up front, and put more focus on getting these devices incorporated into the corporate framework. They could also put in place programmes to encourage employees into going down that route, with sponsored purchase programs, corporate-led deals with suppliers or simply offer those devices as 'perks of the job' during recruitment. This could be run in a similar manner to company car programs where the employee is given an allowance dependent on grade, role and need, but can 'top' it up with their own funds to get a device they prefer.

Whether devices are provided by the organisation or owned by the employee and used to access the organisation's resources, employees have to be made fully aware of their responsibilities. As part of this education process, it is important that employees read and sign up to an agreement that outlines the commitments of the organisation and the reciprocal commitments of the individual. This should include the consequences for failing to adhere to those commitments, for example if employees make illegal or inappropriate use of the organisation's resources.

To maintain control of costs and reap the benefits of mobile working, there needs to be a closer relationship between those responsible for the employee, the technology infrastructure and the money – line of business, IT and financial management. This involves all aspects of the lifecycle; procurement to obtain offers so that those making employee-liable choices avoid paying high consumer tariffs, usage monitoring to ensure billing is accurate and appropriately allocated, and ensuring a clean break when the employee moves on or technology changes.

The challenge for an organisation is not about deciding which route to go down – corporate-liable or employee-liable – but deciding what strategy and policies it needs to put in place to manage cost and risk.



## References

- 1 iPass Mobile Workforce Report April 2011
- 2 Sophos security threat report 2011
- 3 Research conducted by Mozy, part of EMC Corporation, in 2011

## About ttMobiles

ttMobiles is the UK's leading provider of mobile phone management services to companies in the public and private sector. It is independent of the mobile networks and its services work in conjunction with any chosen operator. Its solutions cover mobile phones, datacards, BlackBerrys, home broadband for corporate mobile fleets from 200 – 50,000 devices and were developed to help companies manage the complexities of a rapidly growing community of mobile users and their associated spiralling costs. By implementing its services, its clients are able to gain control of their mobile assets, ensure compliance with internal policies and external tax legislation and deliver cost savings through implementing best practice in mobile management.



## About Quocirca

Quocirca is a primary research and analysis company specialising in the business impact of information technology and communications (ITC). With world-wide, native language reach, Quocirca provides in-depth insights into the views of buyers and influencers in large, mid-sized and small organisations. Its analyst team is made up of real-world practitioners with first-hand experience of ITC delivery who continuously research and track the industry and its real usage in the market.

