



'CONSUMERIZATION' OF IT RESOURCES BRINGS HEADACHES FOR BUSINESS

By Andrew Stillwell

Mobile technology used in everyday life has become the equal to, and in many cases has surpassed, the mobile technology that businesses are giving their employees for work purposes. This has brought unprecedented challenges for businesses as employees increasingly access work email and data from personal devices, and take the lead on demanding which technology they are provided with by their employer. The approach businesses take to resolving this issue will significantly influence their IT policies in the coming years.

With consumer smartphones usage growing rapidly, and with an equally rapid growth in the number of businesses providing smartphones for their employees, there are many 'employed consumers' who now use two smartphones in daily life. Similarity in the form and function of these devices has led to questions regarding the necessity of carrying both and, as a result, there is increasing pressure on company IT departments to either allow employees to use their personal devices for work purposes or to provide consumer-friendly devices.

In a recent GfK survey, 19% said that in addition to their personal mobile phone, they were provided with a mobile phone by their employer. Of this group, 72% agreed they would prefer to have one device that they use for personal and work purposes, with only 6% disagreeing. It is likely that both devices are able to fulfil the tasks required of the other – smartphones provided by

employers have cameras, play videos, and are able to download consumer applications (apps); similarly, work email can often be accessed on personal smartphone devices, company data can be downloaded, and company files opened – so why not just have one device?

As you are probably aware, this issue is more complicated than it sounds: there is significant polarization between the way 'employed consumers' would like to use their handsets and the device security and data management requirements for businesses. For this reason, as the pressure from employees to allow usage of personally-owned handsets for work purposes, or to be supplied with a range of consumer-friendly devices grows, so do the headaches for IT teams as they face unexpected and wide-ranging issues.

.....
 "25% of employed people surveyed admitted using their personal mobile devices to access their work email, with a further 46% saying they wish their company would allow this."

This issue has become known as the 'consumerization' of company IT resources and is widely accepted as the biggest and most immediate issue for those supplying their employees with mobile solutions, and maybe even for those who are not. The way companies respond to these issues, and the policies and protocols that emerge as they do, will have a significant influence on working practices and IT resource requirements in the coming years.

The urgency of this issue is emphasized by the fact that to a certain extent, it is already too late – employees have been empowered by their ability to access work resources on their personal mobile devices through mobile browsers; and are accessing, saving, and sharing confidential data on personal devices and in public spaces to a degree that IT departments had not foreseen and were unprepared for. Indeed, 25% of employed people surveyed admitted using their personal mobile devices to access their work email, with a further 46% saying they wish their company would allow this. This is almost impossible to control, and is giving IT professionals significant policy issues.

There is little doubt what companies would prefer, and what is the most efficient solution – a known list of employees who have been provided with devices using a single OS, which contain uniform software and applications. This would make policy, support, legislation, and budgetary planning transparent,

straightforward, and relatively easy to manage. However, with the increasing number of options available, and the fact that it is now common for employees to have access to personal devices which are at least the equal of what they are provided for work (and to be using these for work purposes), this would be almost impossible to implement.

Therefore, realistic solutions involve either incorporating personally-owned mobile devices into IT systems, or providing and supporting a range of mobile devices which satisfy employee business and personal needs, or a combination of these policies. Don't be surprised if you see a few more grey hairs appearing on the heads of your colleagues in IT!

'Employed consumers' know what they would prefer; 56% of those surveyed agreed they prefer their personal mobiles to their work mobiles, 51% agreed that the features and functionality of their personal mobile is much better than their work mobile (with only 16% disagreeing), and the majority of these only use their work mobile when there is no other option. But do they really know what they are asking for?

The future reality of personally-owned mobiles being incorporated into company IT is likely to be very different to what happens currently. If this becomes official policy, in order to satisfy the data security requirements of their clients, businesses will need their employees to hand over control of sections of their phone and to enable remote device management and a remote wipe facility. In addition to this, it is likely that in the near future, software which segments functions for work and personal purposes and does not allow data transfer between the two will be implemented. Also, businesses may insist on wiping all data from the phone of an employee who leaves. How many employees would be happy to hand over this level of control of a phone which they pay for themselves?

.....
 In the short to medium-term, usage of personal devices to access work email and data will increase, and this is almost impossible to stop. However, this issue could be brought sharply into focus by high-profile cases of confidential or sensitive data being accidentally shared, lost, or passed on by an unwitting employee using their own device.

Equally, although businesses would have a small level of control over mobile devices as they would be used for work purposes, employees would undoubtedly expect support – the IT help desk would become the first stop for all related issues, and would spend much of their day fending off spurious enquiries.

The most likely option looks to be a move towards supporting a limited, but more diverse range of mobile devices than is currently the norm. This would help to satisfy a range of end user needs, but would also allow companies a realistic chance of having the resources to support and maintain them. As consumers become more attached to their mobile ecosystems, employees will want to work with their favored OS or with the apps which most suit their needs – this solution should provide a reasonable compromise between employer and employee.

What will become of personal device usage? In the short to medium-term, usage of personal devices to access work email and data will increase, and this is almost impossible to stop. However, this issue could be brought sharply into focus by high-profile cases of confidential or sensitive data being accidentally shared, lost, or passed on by an unwitting employee using their own device. This would lead to companies implementing more stringent policies, and enforcing increasingly severe penalties for any breach, in order to assure their clients they continue to meet data protection and security requirements.

The recent and continuing increase in company usage of tablets, and personal ownership of these devices, will only make this issue more acute. The potential for tablets to perform a wider range of PC-like functions, and the greater amount of data they will require and store to do this, extends this issue a long way beyond sensitive emails

and attachments. Future usage of tablets will need to be considered both when developing and implementing policy, and when deciding on the handsets which will best serve this policy.

What does the future hold? It is too early to say, and there are plenty of senior decision-makers out there asking themselves the same question. The most likely scenario is a move away from the simplicity that many IT departments have experienced in the past when providing one brand of handset which satisfies all employees, towards a more diverse, but tightly controlled portfolio. What is certain is that IT departments will need to take a lead and set parameters for the provision and usage of mobile devices before their end users become too comfortable with the current status quo. How long will it be before the same employees who are accessing company files on their personal devices realize that someone else is probably carrying sensitive information about them on their handset or tablet, and outrage ensues? When this does happen you can be sure it will be the employers who are facing the toughest questions!

Sources

The survey on consumerisation in was conducted by GfK in April 2011 in the UK. Over 900 respondents were asked about their current usage of work and personal mobile phones and work email accounts and the usage preference amongst those with employer-paid work phones.