

## BYO iPads and iPhones invading your office? Here are the hidden costs

Rob Bamforth, Principal Analyst

### Quocirca Comment

---

In all the talk about the consumerisation of IT, it's the encroachment of consumer mobile devices - in particular smartphones and tablets - that appears to be causing most passion.

The pro argument generally consists of the following strands: employees are already used to better tools in their personal life, we have to do this to recruit a younger workforce, our brand will suffer if we're not seen as leading edge, and it's cheaper.

Whatever the reality or merits of the first three, the last point about cheapness deserves closer investigation along with the impact on organisational security.

The problem is that allowing employees to pick, choose, buy and bring their own mobile tools into the workplace seems like simply outsourcing a particular procurement issue to someone who cares more passionately about it. However, it brings a lot more baggage than the neat little black or white cardboard box the hardware arrives in.

There are three significant aspects to mobile consumerisation - device, contract and content. Device is the part that most focus on, and why not? It's the shiny gadget that has become cool and desirable. It taps into people's feelings about self-esteem and status as well as any social needs for connection or geeky desire for the latest toy.

These devices are expensive so, on the face of it, encouraging employees to BYOD - bring/buy your own device - saves money.

But there are bigger costs and risks at stake elsewhere for the organisation. Mobile devices typically need network contracts, unless relying on pay-as-you-go or free wi-fi for connection.

All-embracing corporate contracts come with many financial economies of scale that a chaotic collection of independent employee ones will lack. Quocirca has explored this challenging issue more fully in its recent free-to-download report "Carrying the can".

The third area, content, is equally complex. Whoever owns and pays for a mobile device - employee or employer - its use is likely to straddle personal and business activities. In addition to communications tools and access for business applications, there will always be a mass of consumer content.

For smartphones and tablets, content includes both software and data. The line is often blurred, and despite many technical and religious discussions, the underlying issues of enterprise control of costs and risks apply either way.

The convergence of work and personal content on one device, no matter who purchased the hardware or pays for the connection, raises the issues of content security, suitability and diligence.

For most organisations, mobile security is a major concern, and rightly so, as it is not only malicious acts such as theft and hacking or the careless loss of a device that might lead to breaches of security. Simply cutting corners for the sake of expediency will not do.

Two doctors were recently overheard on the train discussing how their operation lists were being downloaded to their iPhones. They found it useful but wondered if it might not be good practice, although they presumed there was insufficient detail to identify patients.

Whether this procedure was instigated by the users trying to make their lives simpler or someone in IT wanting to appear useful, is irrelevant. Mobile security needs to be seen to be taken seriously as well as actually being addressed through suitable on-device software, content access practices and services from providers.

All too often it appears there has been only a limited mobile security risk assessment or insufficient user training. These aspects may lack the intellectual pizzazz of security software, VPNs and all things prefixed 'cyber', but the social or human elements are critical for addressing the weakest link - the user.

For mobile devices, even the technical aspects of security are rarely completely understood in IT departments, and the more complex issues involving the diligence of checking suitability of use can really only be answered by those responsible for business processes.

What is the right usage of any given application on a mobile device? It might depend on the individual role or department, work needs, employee location at the moment of access and actual device in use at the time. This is a complex mix of business and social requirements that need suitable policies and tools for enforcement.

Employees should know where they stand, what is acceptable and what is not. There are a number of mobile device-management tool vendors that have stepped into this adjacent area of monitoring, directing and curtailing user behaviours.

While this might seem a bit Big Brother to some, many organisations will need audit trails to show they have sufficient safeguards in place to protect sensitive data. If the details of someone's medical operation were found on the train, blame would be pointed at the health authority or employer first, not the employee.

With BYOD, these management tools now have the more difficult task of projecting the need for organisational control onto the personal device of an individual. They need to do this without compromising the integrity of business activities or violating the individual's personal content or device.

It is a fine line, and an easier way to tackle it would be to have one device for work, one for home - as many do now - but ultimately a portfolio of functions or personalities will need to reside on a single device.

The wave of virtualisation that hit the datacentre is already travelling through the network as virtual private networks and virtual desktop infrastructures. These offer an insight into how businesses might secure BYOD, and may extend virtualisation further into multiple virtual personalities and operating systems on the mobile devices at the edge.

All these developments have cost implications, and these content considerations as well as the contract issues need taking into account when organisations consider the savings of allowing employees to acquire their own devices. Consumerisation is looking as simple and pain-free as convergence.

*This article first appeared on <http://www.silicon.com>*

## 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 markets.

Through researching perceptions, Quocirca uncovers the real hurdles to technology adoption – the personal and political aspects of an organisation's environment and the pressures of the need for demonstrable business value in any implementation. This capability to uncover and report back on the end-user perceptions in the market enables Quocirca to advise on the realities of technology adoption, not the promises.

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 organisations improve their success rate in process enablement through better levels of understanding and the adoption of the correct technologies at the correct time.

Quocirca has a pro-active primary research programme, regularly surveying users, purchasers and resellers of ITC products and services on emerging, evolving and maturing technologies. 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, O2, T-Mobile, HP, Xerox, EMC, Symantec and Cisco, along with other large and medium sized vendors, service providers and more specialist firms.

Full access to all of Quocirca's public output (reports, articles, presentations, blogs and videos) can be made at <http://www.quocirca.com>