

Consumerisation of enterprise mobile devices – is it safe?

Rob Bamforth, Principal Analyst

Quocirca Comment

Just as Mobile World Congress 2011 was about to kick off with lots of pizzazz, hype and fanfare from the mobile industry, many enterprise IT managers would be feeling nervous. Many businesses might have started their love affair with mobile with a few executives innocently picking BlackBerrys, but mobile adoption has now become so widespread, that any security 'niggles' will have a significant impact on a much larger percentage of the workforce.

The upsides of enterprise mobility have been well promoted and, unusually, the reality bears strong resemblance to the marketing hype. More flexibility for the individual, more responsiveness for the organisation and more productivity all round. These benefits are accrued to a greater or lesser extent depending on the nature of the business, type of applications and needs of the business processes that employees are engaged in.

The incremental upside of the positives tends to tail off as deployments widen and business cases become less watertight; however the downsides of scaling up such as managing the end point device itself continue to grow and sometimes escalate.

Mobile security is something enterprises have always been rightly concerned about and Quocirca research studies have often highlighted security as a number one issue for mobile deployments. No wonder, as so many smartphones and laptops are left in the back of taxis or are seen as desirable items to steal and sell on. The risk of data loss from the device through theft or carelessness is one issue; another is the vulnerability of the enterprise itself if an unsecured point of access falls into the wrong hands.

These risks have been well understood for some time, and small families of devices can be "sandboxed" by only issuing to known groups of employees and having appropriate software installed and so kept well under control.

However, early deployments of smartphones tended to be managed in one of two ways – badly, as just phones, leaving big holes, or pretty well, but in a similar way to laptops. The problem is that while smartphones (and for that matter tablets) share many attributes in common with both regular phones and laptops, they are not the same and require more specific controls, especially as they are more likely to have consumer as well as business use.

The numbers of consumer-style mobile devices in enterprise use now, either from official deployment or employees self-choosing - BYOD (bring your own device) – has soared. Not only has ensuring security become harder through this diversity of devices, but also the broader swathe of employee brings a variety of attitudes, skills and experience, many of which will only lead to higher enterprise risks.

At the same time, those with malicious intent will increasingly recognise the growing size of the opportunity from the mobile installed base and the valuable purposes to which they are being put which are diversifying rapidly, from communication, information and navigation to banking, m-commerce and bill payments. These people will increasingly target any weak links in order to gain access to information, or to find ways into the organisation using the device as a gateway.

The value of targeting mobile devices specifically will start to exceed that of targeting desktops. This will eventually result in direct attacks in the same manner that under-protected PCs and their software has been exploited, but also increasingly from indirect approaches such as multi-modal exploits where malware uses a combination of mobile device, traditional desktop and online services.

Another area of concern is the combination of computer attributes, with the associated malware - viruses, Trojans, etc – and those from the telephony world such as the use of SIMs to

attach the device's identity to its user, and non-IP 'telephony' modes of communication such as voice, SMS and MMS. A consequent risk is of mobile smartphone specific attacks that use all methods of communication in concert.

These mobile devices are also highly personal, but in a way that 'personal' computers never really have been. Users tend to trust their mobile phones and believe that they are less vulnerable, when in fact even phone calls can be easily eavesdropped upon (as can be seen with the ongoing News of the World celebrity eavesdropping discussions in the UK). With the explosion in social networking, there is also the likelihood of an old-fashioned 'social engineering' attacks (eg contacting someone and pretending to be the IT department to draw out information) gaining information that can be used for more classical attacks.

The diverse mix of mobile device categories all appear to be doing well in the enterprise domain, which make life even harder for the beleaguered IT manager, especially when it comes to closing down vulnerabilities. Those responsible for ensuring mobile security for their organisations need to become much more vigilant and employ a different approach to the traditional security 'blanket' or firewall.

Essentially the main points of vulnerability – the users – are already on the network, and will need to be channelled down virtually private tunnels, restricted from pockets of data and controlled by automated policy enforcement.

The different aspects of focus required might make it seem like 'herding cats', but there is no retrenching to a mobile world of single platform, corporate issued devices, nor one where employees only use official lines of communication. Mobile devices like smartphones and tablets may seem like small scale mobile computers bringing flexibility to their users, but they bring increasing complexity to those tasking with securing enterprise assets. This will require a dedicated approach to the problem of smart mobile security, and not simply an extension of the traditional IT laptop and desktop approach.

This article first appeared on <http://www.it-analysis.co.uk>

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>