

Straight Talking – Commitment to Mobile Security

By Rob Bamforth, Principal Analyst, Quocirca Ltd

Is your business committed to mobile security or simply involved?

The difference between involvement and commitment is often represented by the role of a hen and a pig in a breakfast of bacon and eggs: the hen is involved, the pig committed. Many employees are increasingly being issued with smartphones, BlackBerries etc. to access their email, or a networked PDA to access form-driven applications, or a wireless laptop to access all sorts of enterprise resources. But are they actively committed to the whole process of keeping the organisation secure, or simply, passively, just involved?

Some might view passive involvement as just fine. After all, if there are tools in place to automatically secure everything without the individual's active involvement, surely that's the best approach?

Outside the realm of IT, many things have moved from active to passive with some apparent benefit. For example modern car brakes using ABS remove the need for a driver to exercise the skill of cadence braking. The braking system automatically applies and releases the brakes to avoid skidding. Arguably some skill has been lost, and drivers are more blasé about the ability of their vehicle to deal with any potential problem of loss of grip, but overall ABS is widely seen as a benefit.

The benefits of taking active decision making away from the individual are not always that clear cut. Take domestic door locks. Self-locking latches may appear to be more secure as they passively lock when pushed closed, but many insurance companies still prefer the positive and definitive engagement of a mortise deadlock, ideally multipoint etc. Anyone who's ever accidentally locked themselves out with a self-closing latch might think then same.

So what does that mean to enterprise mobile security?

While there are ways to offer a lot of protection to the mobile device, data and applications automatically, through anti-virus software, remote kill and wipe, or regular synchronisation, the "it's all safe" approach runs the risk of allowing the individual to abdicate their responsibility.

Getting them involved, committed and taking responsibility when carrying and using the company's assets helps offset the most important mobile security issues – data falling into the wrong hands or being lost through device theft, loss or damage.

But it's not only a benefit from the security perspective. Involving users allows a better understanding of whether a deployment will be a success and deliver the intended productivity gains or not. Not only can users see where the niggling inefficiencies are, but also the productivity is dependent on their attitude and goodwill. Win over their active involvement early and the project should run more smoothly.

That's not to say that IT managers should ignore tools that add layers of protection to mobile data and devices – they should still evaluate them for deployment, as this will help, in some cases dramatically, reduce the risk. However those in the company that tend to believe that security is "somebody else's problem", need to be encouraged to do their part.

It is not only the individual employees; managers too need to review their attitudes. Quocirca research shows that over a third of general business managers do not believe it is important for a security policy to cover the use of mobile, wireless or cellular devices. This type of technology doesn't have to be officially deployed by an organisation for it to be a risk. Multi-gigabyte memory sticks, consumer purchased PDAs and portable hard drives can all be used inappropriately.

The lack of some form of policy is a little too passive an approach. It doesn't need to be a weighty tome, just a simple, well communicated view of the organisation's attitude to security. If you expect your employees to have the right attitude, you have to actively show the organisation is committed too – managers need to recognise their role as pigs, not chickens.

For further details and a mobile security action plan, download the free "Securing the Enterprise" white paper at <http://www.quocirca.com/pages/analysis/reports/view/store250/item3216/>

About Quocirca

Quocirca is one of Europe's leading independent industry analyst firms. One of its biggest assets is the core team of highly experienced analysts drawn from both the corporate and the vendor communities. This team prides itself on maintaining a bigger picture view of what's going on in the IT and communications marketplaces. This allows all of Quocirca's activities to be carried out in the context of the real world and avoids distractions with fads, fashions and the nuts and bolts of specific technologies. Quocirca's focus has always been the point of intersection at which IT meets "the business".

Quocirca Services

The insight and experience that comes from working as an industry analyst as well as a practitioner allows the Quocirca team to contribute significantly to IT Vendors, Service Providers and Corporate clients. To this end, it provides a range of consulting and advisory services. Details of these, along with some of Quocirca's latest analysis, may be obtained by visiting <http://www.quocirca.com>

Quocirca's primary research involves the surveying of many thousands of technical and business end users each quarter, analyzing their perceptions of the possible impact of emerging, evolving and maturing technologies on their businesses.