

BYO security: three ways to tighten iPad and smartphone access without choking innovation

Bob Tarzey, Analyst and Director

Quocirca Comment – Oct 2011

Recent Quocirca research among European, US and Australian small businesses shows how far the trend to consumerisation of user access to IT has progressed. Over 70% of those interviewed said they allowed at least some of their employees to access certain data and applications from their personally own devices.

When Quocirca speaks with chief information security officers (CISO) in larger businesses they admit that one of the reasons their organisations are also observing the same trend is that in practice it is hard to stop. Senior staff will insist on such access, junior ones will seek ways around controls, including the use of other communications channels if they are blocked from access to formal ones, such as corporate email, from the personal devices.

However, as the Quocirca research shows, there are positive reasons for allowing such access. The use of smartphones is fundamental to enabling remote working. Over 90% of the small business managers interviewed had staff that worked out of the office at some point during the week and they were the ones most likely to be using such devices for remote IT access.

Of course, it is not just smartphones. Many of those employees will already have notebook and laptop computers and they are also rapidly turning to tablets. Over 40% of the respondents in the recent research said some of their employees were using such devices and another 20% expected this to be the case within 12 months.

In many cases, remote workers, for example field service engineers logging faults and social workers filing home visit reports, will be using company-issued mobile devices to participate in locked down business processes. However, for a growing majority it is simply about more flexible working and access to information as and when

it is needed – such information workers are behind the mobility revolution that is going on in the IT industry and readers of silicon.com will mostly fit that category.

However, regardless of all the benefits, information workers present their employers with a problem. How do you keep control of the information itself? How do you benefit from mobility and consumerisation without losing control, becoming a victim of data loss and coming to the notice of regulators? There is also a problem for the users themselves. As they switch from one device to another for convenience, how do they get a consistent view of their data?

There is no silver bullet for solving the employer's problem, but there are ways of reducing the risks. First, a business must take as much control of its data as it can. It is possible to secure mobile devices themselves using encryption and host based end-point security, but there is the problem of device ownership; installing software on the users' own devices creates licencing and management issues.

For many, a better way is to impose centralised controls; that is, to provide a means of accessing data which is easy to use and requires minimal modification of the user's device. There are three basic approaches, to achieve its goals a given organisation may need to use one or more of them:

1. Virtual desktops. Here, data is not actually processed on the device, but the device is simply an access tool to a desktop that is available anywhere the user can get online. There are limitations with this approach when it comes to smartphones (due to screen and keyboard size), but software in this area is improving fast (for example Citrix Receiver). However, it may still require some

- locally installed software for some advanced functions.
2. Provide access to applications that allow data to be viewed and updated, but not copied. For example, just because you allow employees to read email remotely does not mean the actual content need be copied to a device. Such applications can be provided through the creation of corporate app-stores that support the range of devices employees want to use and the users can proactively download providing their consent for installation in the process. This is the best way to provide access to corporate applications (CRM, ERP etc.) for those on the move.
 3. Provide direct access to central document stores. Here, with the right products, access can be provided to view files with appropriate caveats. Public domain documents (e.g. market materials) can be freely copied and used later offline, whilst restricted documents can only be viewed whilst online helping to protect an organisation's digital rights. Some products require no local software be installed to provide such access. Offerings here include portals such as Microsoft SharePoint or specific file sharing/backup services such as Trend Micro SafeSync and Druva InSynch.

The last of these also helps solve the employee's problem; if the central data store supports access from multiple operating systems (iOS, Windows, Android etc.) it gives them access to documents from whatever device they happen to be using. Providing this is a secure service it also helps prevent another insidious problem; if there is no easy to use a method for centrally storing documents then employees may synch their devices using other services – some secure, some less so – employers may then have no idea where their data is ending up.

Generally speaking, the benefits of embracing consumerisation outweigh the risks, providing those risks our mitigating in so far as is possible. Employers that are proactive in doing that will ultimately find they get more out of their employees, without taking unnecessary risks with their data.

Quocirca's report; The data sharing paradox, is freely available here:
<http://www.quocirca.com/reports/620/the-data-sharing-paradox>

This article first appeared in Oct 2011 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>