

## Managing information mobility

By Rob Bamforth, Principal analyst, Quocirca Ltd

Managing information is always a challenge. When it's locked inside an individual's head – arguably information mobility in its most basic form – teasing it out and sharing it for the benefit of many rather than the power and influence of one has often proved difficult.

The problem now is quite the reverse. There is such a variety and scope of information, not only the core records that IT systems have captured over the years, but almost anything and everything else has been digitised: images, sounds and video, location and identity tagging, and behavioural data from supermarket shoppers to telephone call records. This is great for data mining and analysis, but the sheer volume of data poses many challenges.

For many it's not, however, a problem of storage capacity – how? – but one of access and discovery – where? – and of containment or security. Storage capabilities have increased dramatically, essentially outstripping the amount of data that has to be stored, not just at the large volume heavy end of data centre storage systems, but at what could be termed the tiny end of storage.

By this we mean the explosion of finger sized memory sticks with one or more gigabytes capacity and portable hard drives the size of a deck of cards holding hundreds of gigabytes. Added to this almost every mobile device from mobile phones to cameras is capable of storing not only its own internal data, but also of acting as an external mobile storage facility.

As information can then become more mobile, keeping it under control is a challenge. Once, taking work home from the office meant risking carrying a stack of papers containing kilobytes of information. In those days, a select few might be permitted to take some files on a laptop, but now almost anyone could carry a bank's entire customer database in their pocket. As more information is condensed into smaller physical spaces, its value is no longer diluted, but distilled and the risks increase.

According to Quocirca research, loss of data through theft or the mislaying of some form of mobile device – laptop, handheld, phone or memory stick – is seen as a greater issue than the problems caused by viruses or the potential for breaches in access security.

This should be no great surprise, but the underlying fears over this loss need to be addressed, as employees and businesses are unlikely to give up the flexibility that mobility brings to their working lives.

The first issue to consider is the shift from perimeter and barrier protection to a shrinking bubble of defences applied directly and proportionately to vulnerable items. In this case, anything that may travel outside the physical confines of the organisation is potentially vulnerable and needs a level of protection.

This does not mean a blanket approach of, say, encrypting everything inside the IT system just in case, but neither does it mean assuming that just because private customer accounts should stay in the building that they will.

A realistic approach to the value, vulnerability and secrecy of various types of information has to be taken, assessing who needs access to what, when and how. It is not enough to ensure that employees will 'do the right thing', as even the most trusted may make mistakes or fall foul of faults in hardware, software and networks, or inadequacies in business processes.

The simple guidance should be, the more valuable the information – where value means not only the value of having it, but also the cost of losing it – the more stringent, complete and discrete the protection should be.

The relationship between the individual and the technology raises the next issue to address, as the small size and simplicity of use of mobile devices mean they are prone to abuse – either deliberately or accidentally.

Firstly, it is easier than ever to bring a small device into the organisation – whether legitimately or not – transfer information onto it, and take it elsewhere. This means organisations should take greater care with access to traditional fixed IT systems and PCs, and should consider products to protect or at least detect when external devices are used, and if necessary only permit the use of corporate sanctioned and managed devices.

This might disappoint the increasingly technology aware consumer-as-employee who wants to use their own better or more convenient technology. However, the organisation has to balance these wishes against protecting its assets.

Outside its perimeters, an organisation is far more dependent upon the diligence of the employee to protect and look after the mobile assets in their care. All too often this is a little lax, and according to Quocirca research, some IT managers would characterise user behaviour as 'irresponsible' as they lose, leave or forget laptops, BlackBerries and mobile phones in taxis, coffee shops, bars and hotels.

This is difficult to stop entirely, so as far as possible protection has to be applied automatically. Beyond that, part of any security policy has to include educating users of their responsibilities, and the consequences of their mistakes.

Overall, the diversity and flexibility of many technologies makes the management of securing information against device loss, or leakage through vulnerable points of access, a far harder challenge. More than ever before, those tasked with applying and managing security policies need tools that streamline the processes and blur the distinctions between different devices, storage systems and access methods, to ensure that common and consistent rules apply to data wherever they are used inside or beyond the organisation.

These principles apply even to organisations that do not condone or provide mobile tools or remote access to their information. The accessibility of consumer technology in terms of price, capability and ease of use means the physical barriers can no longer be relied upon to safeguard an organisation's information, so the focus has to be placed directly on the valuable data and on those who use it.

## 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, Dell, T-Mobile, Vodafone, EMC, Symantec and Cisco, along with other large and medium sized vendors, service providers and more specialist firms.

Details of Quocirca’s work and the services it offers can be found at

<http://www.quocirca.com>