

whiteoaks

Totally transparent PR with proven sales SUCCESS

Computing.co.uk

24 June 2011

computing.co.uk

Keeping data secure in an ever more mobile world

by Phil Dawson

24 Jun 2011

[More from this author](#)

[Be the first to comment](#)



The major data breach experienced by Sony's PlayStation Network has once again led to the thorny issue of cloud security hitting the headlines. In the wake of the incident, alarmist reports have highlighted businesses rethinking their plans to move to cloud-based computing systems. Digital security experts have been quoted as saying that investors, businesses and consumers have put too much faith in the cloud. Computer Associates' general manager for security Mike Denning urged cloud computing service providers to shift their focus from fast deployment to impenetrable and sustainable security.

With the ever-increasing use of mobile devices to access the cloud, these security issues are likely to become even more of a discussion point. Last year, telecoms analyst ABI Research predicted that over 240 million business users would be accessing cloud computing services via mobile devices by 2015.

Further reading

- > Apple should open up iOS within a year, says Kaspersky CTO
- > 84 per cent of UK firms suffered security breach last year
- > The security threat of consumerisation

The growing use of smartphones, Blackberrys, mobile tablets and iPads in the office environment will continue to drive mobile cloud growth. Employees are demanding to use these devices to access the cloud. Yet the devices they use may not be [encrypted](#), may not have appropriate security policies, and may be misused to capture corporate data. Today's smartphones and other mobile devices

are powerful minicomputers capable of storing huge volumes of data and effectively providing a key to the corporate network.

Ultimately, however, none of these concerns are likely to hold back the rapid growth of the cloud computing market, the mobile workforce or of cloud mobility. The benefits of all these trends are ultimately too compelling in terms of their ability to drive business efficiencies, enhanced productivity and greater business agility.

The fact is that there is always some element of risk involved in moving to the mobile cloud. Ultimately, however, there has to be a trade-off of sorts between reward and risk; between the benefits of connected networking and real-time business collaboration and the increased perils involved. And so, it has to be. In making such decisions, businesses may wish to consider what the opposite of the mobile cloud might be. The answer might be a PC sitting in a room in the middle of a military environment that is not connected to any other devices. It is difficult to conceive either of a more secure IT environment...or one less likely to drive business value.

All of these arguments do not, of course, preclude the need for organisations to put in place the most rigorous security systems and solutions they can afford to protect the integrity of their [network infrastructure](#), systems and data. In the case of the cloud, this might include host-based security to protect against [malware](#), encryption, on-device password protection and increasingly mobile device management and access authentication.

It is worth highlighting that no matter how secure the technology, people are still the key to real security. This is important from two major standpoints. First, businesses need to employ IT security experts who understand how the technical infrastructure works and are able to design databases and applications in as secure as fashion as possible.

On an ongoing basis, businesses also need to make sure that secure processes are put in place and that staff are made to follow them rigorously. A key part of this involves engagement and education. If employees do not see security as a top priority, then even the most secure system can easily break down - especially if basic access practices relating to hardware, databases, etc. are ignored by technical staff.

Even with robust technology, there is always a need for high-quality 'human management'. Corporate technologies like secure ID still require a strong bond of trust and a process of involving business and employee. After all, unprofessional or disaffected users all too often pass critical information on

Despite the obvious importance of security, however, organisations must be careful to ensure that by implementing secure systems they are not at the same time, preventing themselves from tapping into the comprehensive benefits that a combination of cloud computing and enterprise mobility can bring. There needs to be a balance between the implementation of secure systems and policies and the ability to drive business efficiencies and ultimately competitive edge in the mobile cloud.

by Phil Dawson, managing director, MDS Technologies Ltd