



**MDS Technologies
Press Clippings Report
August 2011**



Data Center Dynamics
08 August 2011



Keeping calm about security

Phil Dawson, managing director at MDS Technologies, on why he thinks organizations should focus on the business benefits of cloud computing, despite recent security scares

Published 8th August, 2011 by Phil Dawson, MDS Technologies



The issue of cloud security is currently high on the news agenda with the recent breaches at Sony and the International Monetary Fund (IMF) significantly raising levels of concern across the business world and the broader public.



The news that sensitive patient information stored on UK National Health Service (NHS) computer hard-drives may soon be moved to the Cloud has done nothing to quieten these fears. For the next two years, Chelsea and Westminster Hospital will trial an initiative, which involves enabling patients to access their medical records in the Cloud and sharing them with anyone they like, including clinicians or family members.

Storing data in the Cloud aligns with the UK Government's current agenda by helping the NHS cut IT infrastructure, set-up and maintenance costs. However, many fear that this type of scheme could leave itself open to attack following the incidents involving Sony and IMF and the infamous LulzSec clan's recent 50-day hacking rampage, which is said to have included a breach of the NHS network.

In line with this growing trend, a recent survey conducted by network services provider Colt has revealed a surprising level of distrust in the cloud. It showed that 45% of 500 senior IT executives surveyed said they saw security concerns as the biggest risk associated with moving to cloud computing, while 42% said they were concerned about damaging the reputation of their brands as a result of performance or security-related issues.

The growing use of iPads, smartphones, mobile tablets and Blackberry to access the Cloud is unlikely to allay these fears. The issue is that the devices they use may not have the right security policies, may not be encrypted 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 – if placed in the wrong hands.

None of these concerns are likely to hold back the rapid growth of cloud computing and nor should they. The benefits of the Cloud, in terms of its ability to drive business efficiencies, greater business agility and enhanced productivity, are too compelling for businesses to ignore.

Businesses need to accept that there has to be some element of risk involved in moving to the Cloud. There always has to be a trade-off of sorts between risk and reward; between the benefits of connected networking and real-time business collaboration, enhanced productivity and the increased dangers involved. Ultimately, it has to be the decision of the individual business as to how far down the road to full cloud computing they wish to travel.

In making their choice, they may wish to consider what the opposite of full cloud computing would 'look like'. The answer might be a PC sitting in a concrete-encased room in the middle of a military environment that is not connected to any other devices. It is difficult to conceive of a more secure IT environment...or one less likely to drive business value.

In any case the security concerns of cloud computing have been hugely overplayed. Rob Lovell, chief executive of ThinkGrid, claimed recently that "a lack of understanding" about how cloud computing works is responsible for many firms' reluctance to embrace the model. He noted that business leaders who lack an understanding of hosted services tend to be more worried about the security issue. "When they understand that data is stored remotely in the cloud and is managed by a specialist company with a highly skilled team of IT professionals, it is actually far more secure than their typical office IT set-up," Lovell said.

People and processes

Of course, these arguments should never negate the need for organizations to put in place the most rigorous security systems and solutions they can afford to protect the integrity of their data, systems and network infrastructure. Nevertheless, no matter how secure the technology implemented, people are the real key to security. This is important from two major standpoints.

First, businesses need to employ IT security experts who understand how the technical infrastructure works and can design applications and databases in as secure as fashion as possible. Second, organizations need to ensure that secure processes are put in place and that staff are made to follow them rigorously.

A key element of this is the need to put in place a process of education. If employees do not view security as a priority, then even the most secure system can break down - especially if basic access practices relating to hardware, databases, etc are ignored by IT 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 between business and employee. After all, unprofessional or disaffected users all too often pass critical information on passwords, codes and ID numbers to others.

Despite the obvious importance of security, however, organizations 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 cloud computing 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 cloud.