Cloud computing: as safe as houses

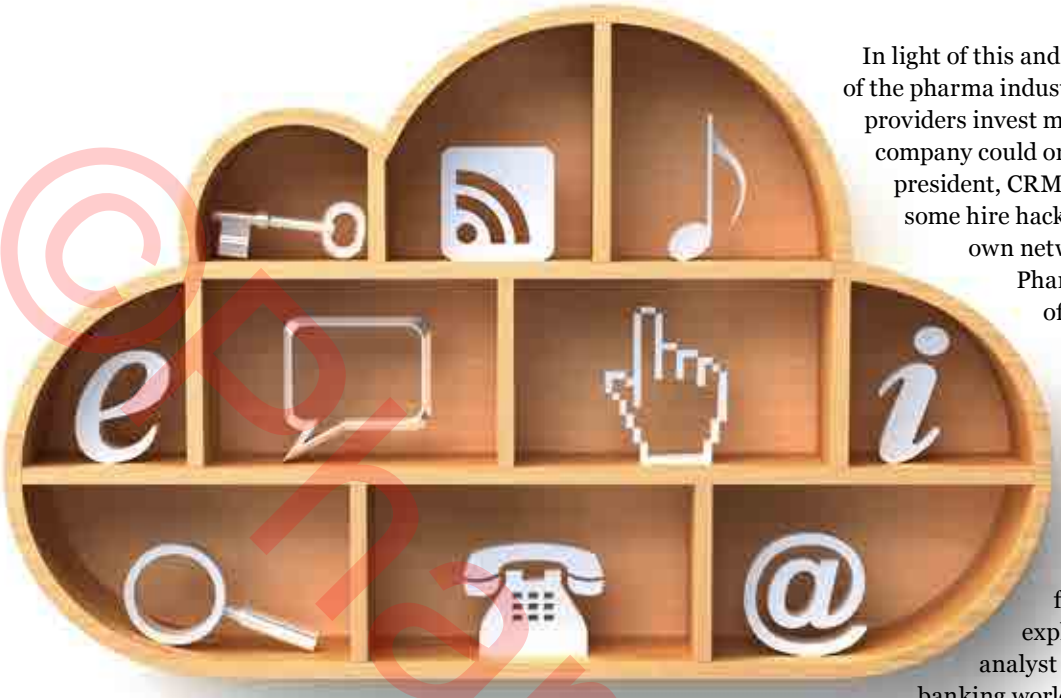
The rise of cloud computing as a means of storing and accessing data is proving a real "innovator's dilemma". Can it ever be as safe as in-house storage and is the public or the private cloud better?

Senior Reporter **Katrina Megget** | Edited by **Jenny Hone/Claire Bowie**

Is it any wonder the industry is hesitant about dipping its toes into this new area of pay-as-you-go IT? As George Waidell, life sciences expert at IntraLinks, points out, a healthy amount of caution is necessary – with both the corporate social responsibility aspect and the intellectual property of the product pipeline to protect – "the lifeblood of pharma", as Waidell puts it. "Even one breach," he says, "could negate or significantly impact the market opportunity for that product." However, many moving into this space say the security concerns shouldn't be a roadblock to leveraging the numerous time, cost, storage and collaborative benefits of cloud computing.

R&D information tends to induce the most concerns when it comes to cloud security, meaning many shy away from this, preferring instead to put the less risky sales and marketing activities into the cloud. Indeed, Mike Askew,

©PharmaTimes



managing director at Data Intelligence, says he has also noticed a trend where companies are preferring the cloud for business intelligence and customer relationship management solutions for this reason. However, Sejal Amin, vice president life sciences technology at Thomson Reuters, says the security concerns surrounding R&D can be addressed. "With proper monitoring, R&D should be able to live on the cloud along with sales and marketing activities, with little or no risk of being infiltrated by hackers or other malicious third parties."

Yet it is quite a transition for an industry used to keeping a tight rein on its information to have a third party vendor handling your sensitive data, notes Mike Stroukoff, GlaxoSmithKline's director of cloud architecture. "We used to be able to rely on firewalls and physical walls around our data centres for reassurance, now we need to expand our capabilities to ensure the same level of safe operation in the cloud. Where do you feel more in control of your children's safety?" he asks as an example. "When they are playing in your basement or when they are at a friend's house?"

Certainly, the NHS' recently publicised security breaches – between March 2011 and February 2012 it was responsible for more than a third of the 750 or so cases of lost data or hardware in the UK – have done little to promote confidence in IT security. But many suggest the security issue is more molehill than mountain and point out that cloud computing could provide more control and security than traditional in-house IT systems.

"We find many examples," says Waidell, "where content is still shared for collaboration or review via file transfer protocol, email, paper and fax. But once the document is outside of a system it is impossible to revoke security access or even track that it has been viewed by the intended user." Amin agrees: "Physical security doesn't guarantee safety – a single copy can walk out the door just as easily from an unsecured workstation."

In light of this and the stringent security needs of the pharma industry, many cloud-based service providers invest more in security than a pharma company could on its own, says Paul Shawah, vice president, CRM strategy at Veeva. "For example, some hire hackers to attempt to break into their own networks to identify any weaknesses. Pharma companies don't do all of this."

Askew agrees: "In reality there can be more risk from the use of USB sticks, unsecured internet connection and less than honest employees. Service providers' reputations and corporate capital hinge on security, so the stakes are high for them." Look at online banking, explains Jeremy Poland, growth analyst at Cello Business Sciences. The banking world has been able to overcome the security issues "with the use of highly secure servers to host data, with users accessing services using a unique ID and strong password".

One pharma company to embrace the cloud is Bayer HealthCare, which is currently using and evaluating cloud computing for various applications. According to Matthias Moritz, head of organisation and information at Bayer Healthcare, "Bayer is keen on having security built into all layers of IT regardless of either the hosting platform – cloud, virtual or physical servers – or the provider. As with any technology," he adds, "we have to understand how we can benefit from its advantages while adequately managing the risks."

The private cloud

For some, of course, the "private cloud" offers a more secure option – "a gentle introduction to the cloud", describes Nick Lynch, external liaison officer at the Pistoia Alliance, a pre-competitive alliance of life science companies and academia. In short, the private cloud is the virtualisation of data dedicated to a single entity or organisation, often only accessible by invitation. By contrast the public cloud is an environment for sharing information between multiple users. So is a private cloud a more secure and safe haven for R&D data? "Many say the private cloud is just a new way of saying data centre," says Amin. "In this respect, it can be a good solution for the pharma industry. However," she adds, "this model is expensive and as such negates a lot of the value of the cloud-based model if used as a 100% solution."

Likewise, Waidell suggests the private cloud doesn't necessarily fit in with industry's increasing move towards collaboration. There is also less flexibility, with the potential for "overload", and increased burden from individual URL links and multiple passwords, he says. Furthermore, "a private cloud may be considered to be 'under the radar', potentially leading to corners being cut on security options".

©PharmaHired

“The key is to be able to leverage the potential of the cloud to enhance productivity while at the same time maintaining focus on patient safety and managing delivery risk”

Indeed, Shawah suggests the public cloud is more secure precisely because of its multitenancy. “Multitenant application providers can keep all their customers up to date with the latest and greatest security measures. Conversely, within the private cloud, companies need to manage upgrades for private cloud applications on their own... Because the pharmaceutical industry changes so rapidly and companies are obligated to comply with changing industry regulations, the public cloud is the best choice for pharma companies. It enables them to keep up with frequent upgrades, enhancements and regulatory changes that are only possible to deliver cost effectively on a true multitenant architecture.”

Best of both worlds

Nevertheless, companies will undoubtedly remain hesitant about putting all their data into the public cloud. The hybrid approach, which mixes the private with the public cloud, may therefore be the way forward – or as Stroukoff says, “essentially a transition state between where we are today and where we’d like to be tomorrow”. Indeed, he points out this is the “more suitable model” for GlaxoSmithKline. “We can leverage a hybrid model to quickly get the low-lying fruit while planning more thoughtfully about other opportunities to move into the cloud.”

While the hybrid approach is shunned by some purists, Amin believes it provides the “best of both worlds” for pharma by ensuring sensitive data stay ‘in-house’. “Through the use of hybrid, the organisation can control how much to share with partners. It can use the platform to combine content and analysis to lower the barriers to innovation by improving the interoperability of the R&D business processes.”

But at the end of the day, the key is to be able to leverage the potential of the cloud to enhance productivity while at the same time maintaining focus on patient safety and managing delivery risk, says Jim Kendall, vice president, information technology, client services at Quintiles. With so much at stake, Kendall says it is important for companies to negotiate a due diligence process when assessing cloud vendors.

“We have taken a proactive approach,” says Stroukoff, “and are driving towards a universal GSK security model that provides single sign-on, federated identity management and central claims management. To mitigate our risk as we move forward, the use of this model is becoming a non-negotiable requirement in the cloud vendor process.”

Waidell agrees that much of the onus for security falls on the providers’ shoulders, saying it is important for pharma companies to evaluate the vendor’s cloud security – auditing its processes and controls, understanding its security testing and methods, and identifying the risk assessment and management methods. “At the end of the day, for cloud computing to be successful, the industry needs to look at security as a core value and solutions that are provided should not compromise that.” Furthermore, Lynch says it’s also down to providers to consider the needs of the pharma business model and provide solutions to increase adoption and break down barriers.

Cloud computing is yet another new technology for pharma to consider, but security concerns should not hold the industry back. As Amin says, “cloud computing should not be ignored because companies that are able to embrace the benefits of cloud computing will innovate faster, and at lower cost, than their competitors.” **PT**

©PharmaTimes

Veeva CRM
The multichannel cloud platform you’ve been searching for.
eu.veevasystems.com