



15 MINUTES with PARSH MISHRA

VP Technology Infrastructure - WHG Compliance, Citigroup

Parsh Mishra works for Citigroup Technology Infrastructure on the Risk Management side. The foremost function of his team is to bring down IT inherent risk to tolerable or non-affecting levels.

ITO America: For many executives, jumping into cloud computing means weighing the potential security risks against the decreased operating and maintenance costs. At this point in the game, which one is winning out in your mind?

Mishra: There are certain tempting benefits of cloud computing that make you ponder over or weigh risk versus benefits. We have heard that “cloud computing is wonderful, but it is very risky.” The question that pops up is: how to align these two elements? It all depends on how cloud computing serves one’s needs and the expected outcomes out of it. Cloud computing is not for all and sundry. Therefore, I believe that both risk versus benefits come into play depending on what one wants to achieve with cloud computing.

In today’s recessionary market, the IT sector has been badly hit due to budgetary and spending constraints which is also one of the primary reasons that is cloud adapters are holding back, mainly because mitigation of risks costs money. However, there are certain areas where the dedicated IT department is not deemed necessary and cloud computing can play a pivotal role in such areas. There are also

areas where there are no security risks and cloud computing appears very attractive because cloud solutions provide the power of supercomputer at a fraction of the cost with no upfront capital costs. Above all, the core area of IT is still hesitant to move to cloud computing due to the underlying security risks.

ITO America: What, in your opinion, are the biggest security concerns in the cloud?

Mishra: Cloud infrastructure security is the biggest security concern in cloud computing today. There is constant worry about “information malpractice” as you lose control once it is handed over or moved from your area to the cloud. Your data sits besides your competitors’s data.

Cloud computing may be on the corporate agenda of many companies but the security risk is delaying them from going to the mainstream, particularly cloud infrastructure security.

ITO America: When considering the public cloud versus a private cloud, do the security concerns differ in any way?

Mishra: Yes, it differs to a great extent. The public cloud is mainly used for the purpose of storage among others. It essentially uses shared storage. There is nothing shared in the private cloud computing environment. It is completely custom designed. Private cloud provides robust security on top of good performance. Hence, private cloud is considered when performance and security are of utmost concern.

ITO America: Do you believe that the recent hijacking of Google’s web-based Gmail will deter businesses from entering into the cloud?

Mishra: The idea behind cloud computing is to have data as well as application reside on the Internet rather than on your computers. This has certainly caused paranoia on certain sections and this is expected. If you look at this attack, it was

directed towards “technology infrastructure.” It is no way an attack on cloud computing. In this attack, malicious software was used to infect PCs that lead to the main attack. I don’t consider this an assault on the cloud computing directly.

ITO America: Have you run into any compliance issues while working on cloud computing projects at work/practices?

Mishra: On one hand, there are some key regulations like SOX, PCI DSS and GLBA among others that have specific requirements. On the other hand, security controls are applied by the cloud service provider. I have found that cloud service providers are not forthcoming when it comes to providing information on applied security controls. At times, it becomes very challenging. In the absence of this, it is hard to conduct the gap analysis between the regulation requirements and applied security controls. These control assessments are not a one time process, and the assessment should be ongoing. I recall a classic case where the cloud service provider denied conducting the vulnerability assessment.

ITO America: What advice can you give to executives who are considering cloud computing for their organization?

Mishra: It holds a promising future. The executives should invest in it because of multifarious benefits both in the short and long runs. Before embarking on it, it is essential to have a broad plan, taking into account the security, compliance and privacy. On the basis of security, compliance and privacy of data, one should choose the right model that suits one’s organization. The broad planning is of utmost importance.



www.itoamerica.com