Guardians of the cloud

Posted At : July 26, 2011 3:31 PM | Posted By : Derek Johnson
Related Categories: Technology Trends, Information Security, Outsourcing, Emerging Technologies, State & Local, Procurement, Government Reform, Financial Crisis

Cloud computing applications and solutions continue to be one of the hottest trends in the public and private sector today. This should come as no surprise to anyone who has paid even marginal attention to the government contracting market over the past two years. Going to the cloud is **often cheaper, more efficient and easier to maintain** than traditional software, email and storage options. At a time of shrinking budgets and drastically reduced prospects of federal aid, state and local governments are clamoring to implement cloud solutions where practical in order to start reaping financial benefits as soon as possible.

"Where practical" are the operative words in this equation. Information technology departments and their CIOs are anxious to utilize the cloud, but not if it means exposing their records and data to lower security standards. **According to a November 2010 survey** of 460 government officials by the 1105 Government Information Group, more than half (55 percent) of those surveyed believe cloud solutions are not secure enough, while nearly three-fifths (59 percent) believe traditional IT solutions are safer. **A 2011 survey of U.S. business and IT professionals** by the Information System Audit and Control Association found that almost half (46 percent) of respondents reported not using cloud computing at all or only for non-mission-critical functions. The number of respondents who believed the risks of cloud computing outweighed the benefits (41 percent) was twice as large as the group that believed the reverse (20 percent).

While concerns about security have diminished as stakeholders learn more about the technology, and industry leaders begin to address those worries, "is it safe" continues to be the number one question asked by governments after "how much money will this save us?" Vendors have to be able to provide satisfactory answers for that first question before they try to hook governments on the potential of the second.

Dr. Nir Kshetri, associate professor of business administration at the University of North Carolina at Greensboro and author of "The Global Cybercrime Industry: Economic, Institutional and Strategic Initiatives," believes the problem lies in a combination of factors. First and foremost, cloud computing is still a nascent technology. Businesses are shy about implementing services they don't fully understand, and governments are even more cautious. For many government IT managers, "going to the cloud" stops at email and instant messaging. Furthermore, the IT industry as a whole has yet to provide the kind of support infrastructure that protects older technologies.

"The cloud is not a familiar terrain for most IT security companies," said Kshetri in a recent interview.

Storing data in the cloud as opposed to your own personal facilities (where security strategies are more straightforward) has a "wild West" component that makes IT managers nervous. **As a Global Knowledge white paper on cloud security** puts it, cloud computing "blurs the natural perimeter between the protected inside and the hostile outside."

This brings us to our second problem: lack of industry standards. It's not that the market hasn't made an effort to address these issues; there is no shortage of **organizations**, **IT security firms**, **industry associations** and **formal certifications** dedicated to establishing best practices when it comes to cloud safety. So far though, the market has yet to coalesce around a universally-accepted definition of what constitutes "safe."

Kshetri believes that despite the clamor for safer cloud solutions, IT vendors haven't done enough to assuage the fears expressed by the public and private sectors when it comes to security.

"Surprisingly, IT companies individually do not seem to take serious measures to address their clients' concerns related to security and privacy. They are investing too little in improving security practices," he said.

Finally, the ambiguous nature of storing data in the cloud can carry a host of jurisdictional legal issues that governments are not eager to explore. An American business or government that entrusts its data to a cloud vendor with servers in Germany may be walking into a murky legal situation in the event of a security breach.

"The cloud-related legal system and enforcement mechanisms are evolving more slowly compared to the technology development," said Kshetri. "Privacy, security and ownership issues related to data stored on cloud currently fall into legally gray areas."

Analyst's Take

It's easy to make the case that cloud computing's potential is so promising, governments will be forced to come around to the concept of implementing large-scale, comprehensive cloud solutions in the near future. Indeed, a perfect storm of problems may push many uncertain state and local governments into the cloud over the next few years. The 2011 fiscal year was marked by massive budget cuts and workforce layoffs, with more to come in 2012. No matter how the current federal debt-limit drama plays out, state and local governments will feel the crunch. Either huge slashes in spending will leave states and municipalities fighting over an ever-shrinking piece of federal-aid pie, or the collateral impact of U.S. default will **lead to a collective downgrade in thousands of municipal credits and municipal debt**. In addition, 2011 marked the last trickles of federal stimulus aid that has kept many state and local governments from considering even more drastic measures.

Nonetheless, even if the future does lie in the clouds, there is real evidence that the inability to seriously address security questions is slowing this transition and turning what should be a no-brainer into an exercise of risk and tradeoffs for CIOs. The real market for cloud computing lies not in the governments that have already dipped their toes into the water, but rather the vast number of towns, cities, counties and states that are lined up to dive in once they're convinced it's safe to do so.

With that in mind, here are five tips to incorporate into requests for proposals (RFP) responses:

1.) Eliminate or reduce worries about control

Most of the specific concerns government officials express about implementing cloud solutions (How safe is information if it's just floating out there? What happens if there's a disaster?) can be traced back to a simple emotional thought: I don't have control over my data and that makes me uncomfortable. Find ways to eliminate or reduce those concerns by tailoring solutions that provide governments with compartmentalization options, detailed backup recovery plans and sole access to data encryption keys. This can sometimes be tricky, but a state/city IT department will be much more willing to jump from the plane if it gets to pull the parachute cord.

2.) Clearly define the geographic location of your data centers

IT managers want to know where the other side of the rainbow ends with cloud storage systems. The last thing a CIO needs to worry about is whether his or her state's tax information falls under American or Chinese jurisprudence because the cloud vendor was unclear about where they ultimately store client data. "I don't think that there are clear regulatory frameworks developed for these issues right now," said Kshetri. "Government organizations may minimize the risks by specifying in the contract as to where the data needs to be stored. If the contract doesn't explicitly mention that – under the current regulatory environment – it could be a very complicated issue."

3.) Get a stamp of approval

As stated before, there are currently no universally-accepted industry standards for cloud security. That does not mean vendors shouldn't seek some form of accreditation to present to procurement offices. Undergoing one or more **certification** procedures can help a cloud provider stand out from the crowd while waiting for governments and businesses to settle on industry norms.

4.) Set up a viable customer service infrastructure

Surveys have shown that a poor understanding of cloud computing is directly related to increased security fears. Cloud solutions should have a built-in component that provides support as well as education to government clients. This **typically has not been an area of strength** for cloud providers in the past, and it has not gone unnoticed. As Yankee Group Analyst Camille Mendler said in an interview with DefenseSystems.com: "Cloud vendors offer poor service guarantees and limited financial redress if their service fails. Get-out clauses are rife, and robust privacy policies are rare, potentially exposing organizations to litigation."

That perception of unaccountability in the face of disaster is what scares most governments out of experimenting with cloud computing on a larger scale.

5.) Stay in your niche!

Government agencies handle different types of information. Storing state tax information carries a different set of regulatory obligations than Medicare and Medicaid patient records. Casting a wide net may increase your pool of business opportunities, but ultimately, health departments are going to contract with vendors that have an **established background of providing cloud solutions specific to their field**.

Cloud computing technology is still so new that no matter what your company chooses to specialize in, there will continue to be a vast, untapped market of state and local governments looking to make the leap over the next five years.