



## Put security, savings on par in cloud

By Vivian Yeo

Wednesday, August 05 2009 07:06 PM

SINGAPORE--Organizations venturing into cloud computing ought to put security considerations on par with cost savings realization and ask "hard questions", according to a security expert.

Cloud computing and the idea of shared infrastructure is a great cost savings construct, but organizations need to evaluate how their vendor can answer two questions in tandem: "Can these guys really save us the money; if they can, can they do it securely", Philip Dunkelberger, president and CEO of PGP Corporation, said Wednesday in a media briefing.

PGP is a charter founding member of the Cloud Security Alliance, which put forth a best practices guidance document in April.

"[In trying to balance] efficiency and economics in a very tough economic time, I think what might suffer--if people aren't careful--is the security of the data you're passing between the cloud provider and your own environment," said Dunkelberger.

He added: "You don't want to lose all your cost savings by having a data breach [and] by getting into a costly jurisdictional battle over the right of government to review the data you might be storing in somebody's data center, and who has access to it."

According to Dunkelberger, the security capabilities of current cloud computing providers range from "excellent to poor". Cloud players that truly understand security concerns have comprehensive plans, while others simply point to service level agreements. "There's a big distance between somebody specifically telling you how they are going to protect your data, and somebody saying it's in the contract," he pointed out.

Some issues that a cloud vendor needs to address before an organization jumps onto the cloud computing bandwagon, are the security issues with federating data in a number of data centers in different jurisdictions; the kind of data that should be put on those servers, who has access to it; what processes, procedures and technology are in place to secure information; and what happens when data is breached.

Cloud computing providers can and should answer those questions, he said. That could cost them money, which may mean that they would have "to give up some of the cost savings, and charge customers for extra security".

On the other hand, businesses need to have proper security plans and management in place. "If you are not protecting data from the get-go, you shouldn't be putting your data on the cloud," Dunkelberger said.

### **Beware that janitor**

A common security loophole for businesses is the failure to monitor access to corporate information. Third-parties such as outsourcers, temporary workers or contractors are among the biggest threats to sensitive or confidential data, Dunkelberger pointed out.

Businesses really need to be vigilant about who has access to information, he said. In a world of cyberespionage, the janitor with access to every single part of the building has become the "most powerful person", he noted.

Citing PGP-sponsored research released in February, Dunkelberger added that breaches caused by third parties generally cost more. The average cost of a record breached by third-parties is US\$231, while the loss of a record as a result of an organization's fault cost US\$202 on average.