

[Print](#)

Cloud security raises unanswered security questions

Cloud computing is a promising evolution of some old ideas, but some security questions remain unanswered

10/19/2009 3:46:00 PM

by Grant Buckler

We've been hearing a lot about [cloud computing](#) for the past few months, much of it hype. This is one of the year's hot buzzwords, and every marketing type on the planet wants a piece of it. So a lot of what the cloud label is attached to isn't really new - it's just a new name slapped on software as a service, managed service providers or, if you're old enough, the service bureau.



This isn't to say there's nothing to the idea. Cloud computing is a next stage of evolution, taking those ideas a little farther thanks to technology we have today that we didn't have five, 10 or 30 years ago.

Hype will fade, substance will remain. That's normal. It's also normal that in the midst of the hype, real issues and problems don't get the attention they should. One of those issues is security, as Christofer Hoff pointed out at the recent [SecTor conference](#).

Hoff is currently "doing nothing until he finds something more fun to do or his wife goes mad and sends him to Starbucks to pretend to work," as his SecTor speaker bio puts it. But he was chief security architect for Unisys and chief security officer at Western Corporate Federal Credit Union, among other security-related positions, and it seems his definition of doing nothing stretches to being fairly active on the speaker circuit.

He told a good-sized audience at SecTor's opening keynote that cloud computing as it stands today has some significant security pitfalls.

Questions have been asked about [cloud security](#) from the beginning. You put your data out there on some server somewhere - you may not even know where - and how do you know it's secure? One of the most convincing answers to this has been that if you're an average small to medium-sized business your data is quite likely more secure in the hands of a big sophisticated technology company than it is on your own servers, because outfits like Google and Amazon know a lot more about security than you do.

True in principle, but as Hoff pointed out, the cloud providers generally don't take full responsibility for securing their customers' data and applications. If they provide basic infrastructure, securing the applications you run on it is "pretty much all up to you." The classic software as a service model comes with more built-in security, but it's the customer's job to ensure contracts provide adequate protection.

Cloud computing doesn't make existing security issues go away, Hoff argued, and at the same time it reduces the amount of control companies have over their data and applications.

This doesn't mean cloud computing is snake oil. Striking a hopeful note for a moment, Hoff did say that there are quite a few really smart people working on the problems.

But he also told one story that should make everyone stop and think. Seems the FBI was investigating a company that used a Chicago-based cloud provider, and wanted the company's data. So the agents showed up at the data centre. But nobody could just take them into the data centre and say "that company's server is that one over there." The data was spread across multiple servers and storage devices also used by other companies.

You guessed it. The FBI just took them all. There are issues that need attention here.

[Print](#)[Close Window](#)