

The big dilemma

Security versus scalability in the public cloud

By Larry Lange

Enterprise executives identify security as the biggest risk of the public cloud, so it is not surprising that they overwhelmingly—about 8 to 1—prefer private cloud over public for their IT infrastructure, according to the PwC IT Outsourcing and Cloud Computing Survey.

What is somewhat surprising is the amount of push back on this finding from vendors of IT outsourcing (ITO) and Infrastructure-as-a-Service (IaaS). ITO and IaaS executives, who reviewed the survey findings, agree that the customer’s biggest concern is public cloud security. But they argue that the concern is more perceived than real, that the public cloud will be part of the future IT infrastructure environment and that it will happen much sooner than customers think. Their companies can meet current demand for private cloud services, but they say limits to scalability and scope in private clouds eventually will spur enterprises to adopt hybrid models with private and public cloud elements.

Here’s what the survey of executives at almost 500 companies found on these issues:

- 62 percent rated data security as a “serious” or “extremely serious” risk to IT infrastructure in the public cloud. Four other risks were essentially tied as a distant second, each in the low 40 percent range. (See Figure 1)

- 57 percent said the more secure private cloud, restricted to a single enterprise, either internally managed (25 percent) or externally managed (32 percent), would be the best way of managing IT infrastructure in three years. A mere 7 percent said the public cloud.

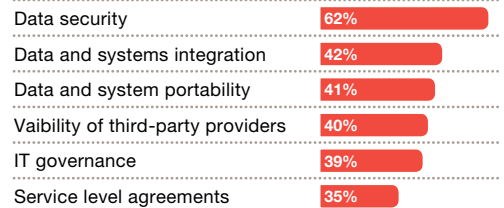
Figure 1: Perceived risks in the public cloud

Question

Please indicate your view on the seriousness of each public cloud risk for your organization, on a scale of 1 to 5.

- 1 = minimal risk
- 3 = moderate risk
- 5 = extremely serious risk

Percentage of respondents who indicated a 4 or 5



n = 481

- Yet, as the second part of “Best versus reality” illustrates, more IT resources will still be allocated to traditional methods in three years, ranging from an average of 39 percent still in the internally managed data center to an average of 7 percent in the public cloud. (See Figure 2)

Clearly, most enterprise IT strategies are likely to be mixed and will include a hybrid of private and public cloud for some time to come.



William Beer
Leader in PwC’s London
Information Security practice

William Beer, a leader in PwC’s London Information Security practice, says it is not unexpected that enterprises and service providers see the security issues of cloud computing differently. “While there are some common requirements at a basic level for information and data center security, the reality is that industry sectors, individual enterprises within sectors and even different geographies all have unique security concerns. The nature of cloud computing, especially public clouds, is shared infrastructure—meaning a one size fits all approach. This may not graph well onto the complexity of information security requirements,” Beer says.

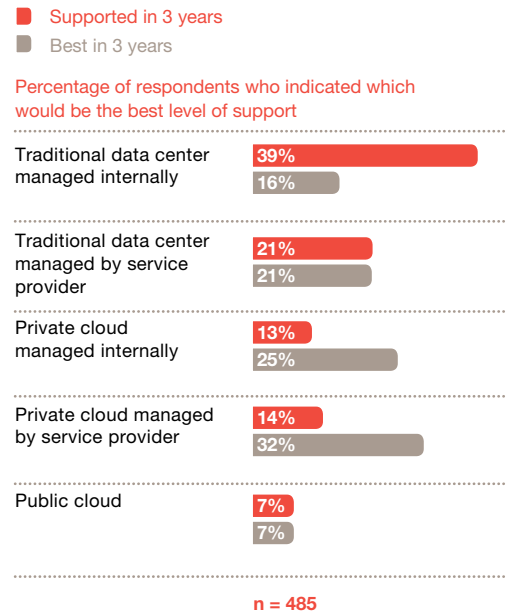
Clients do evaluate which mission critical applications could run safely in the public cloud, but their choices show a “strong preference for private cloud,” says Siki Giunta, global vice president for CSC, an ITO provider. Nonetheless, she expects the hybrid cloud to displace the internally managed traditional data center over the next five years. Through their experience, she explains, customers will learn that security and transparency are well handled in the public or off-premise setting, and this will, over time, prove that off premise can be as secure as on premise.

57%
Survey respondents who indicated that a private cloud is the best IT solution in 3 years

Figure 2: Best versus reality in three years

Question

Which do you consider will be the best solution in 3 years? How much of your IT infrastructure will be supported by each of the following in 3 years?



John Keagy, executive chairman and founder of GoGrid, an IaaS provider, says the private cloud is popular now because customers have fears about the public cloud due to security, compliance and legal needs. Eventually, he says, “They’ll run into a lot of problems with workloads that shift by the hour, with scalability, programmability and agility,” and then begin to shift to a hybrid model that includes the public cloud. The public cloud “can be used on demand, pay-as-you-go, no long-term contract associated with it and almost no penalty if you decide you don’t need it anymore.”

Keagy also points out that a private cloud run in the enterprise’s data center still means the organization must own the equipment, hire staff and bear the operating costs.

The market will increasingly demand hybrid environments.

Jody Little, vice president of cloud portfolio at Fujitsu America, an IaaS provider, says the first step for many customers would be a managed private cloud because that would still offer control over their infrastructure. She sees the private cloud as a “stepping stone” to the managed hybrid model. “That’s where cloud will probably go over the next five years,” Little says. “The market will head to more of a hybrid environment.”

As the “Best versus reality” graphic shows, survey respondents said an average of just 14 percent of IT resources would be allocated to private clouds managed by a service provider in three years, and just 34 percent across all cloud options. This and other findings from the PwC survey suggest a gradual migration to all cloud options; in contrast, the vendors predict much faster adoption.

For example, based on conversations with large enterprise clients, Robert Boles, senior vice president and head of global IT infrastructure services at Cognizant, an ITO provider, expects that 50 to 80 percent of these enterprises’ application portfolios will move to the cloud in three years. The majority of these applications will be deployed into private clouds, with some portion taking advantage of public or hybrid cloud offerings.

Within three years, “60 to 70 percent of interested cloud customers will be on the public cloud,” but as part of a hybrid model, says Venguswamy Ramaswamy, global head of iON, the cloud services unit at Tata Consultancy Services.

CIOs are also concerned about compliance issues, which are important because most providers, both ITOs and IaaS vendors, house data in various locations—and not always in the region the customer is headquartered.

“European laws are especially strict on data protection, some mandating the data must reside in the country of origin,” says Fujitsu’s Little. “A lot of cloud providers are not able to guarantee where a particular client’s data is going to reside and to prove that for governmental audit purposes.”

These executives think the security fear will dissipate sooner rather than later as the benefits of flexible capacity and significant cost savings become too tempting to ignore. Even so, customers are likely to want a “management wrapper around the public cloud offering,” which Cognizant can provide, Boles says.

Dell, a new IaaS provider, will launch a managed hybrid cloud offering later this year, says Mark Bilger, the CTO. “If you need more capacity, our solution will seamlessly burst from your private cloud to the public cloud.” Dell will provide a management layer around such public cloud capabilities, he adds.

Bilger thinks security is not a “substantive issue anymore, but of course, it’s a perception issue, and will continue to be so for many years.” He believes trusted vendors with established security technologies, like Dell and large ITO providers, will ultimately assuage the worries CIOs have.

64%

Survey respondents who outsource IT that say data security in the cloud is a serious risk

There's little evidence in the survey that providers have convinced their own customers yet: 64 percent of ITO customers said data security risk was "serious" or "extremely serious," compared to 58 percent of non-ITO customers; and 61 percent of respondents who developed a cloud strategy with their ITO partner said data security risk was "serious" or "extremely serious," compared to 57 percent of respondents who developed a cloud strategy on their own.

As vendors begin to recognize the commercial importance of implementing robust information security, PwC's Beer expects a gradual reduction of these concerns among CIOs. "In reality, the public cloud infrastructure option is less than five years old," Beer notes. "Public cloud computing and third-party vendors are hearing these concerns from potential customers and responding with new technical solutions and, more importantly, better governance.

But information security is not a domain where enterprises can adopt incomplete solutions, no matter how advanced they may be and how attractive the cloud option is from a cost perspective. Unlike the adoption of, say HTML5, where new functions and features can be tried incrementally, new approaches to protecting data and infrastructure must be relatively complete from the get go."

The security issue is not likely to go away soon. CIOs will continue to be wary as long as the IT world suffers the occasional headline-grabbing breach like this year's reported hacking into an online video game network, which is hosted in a leading public cloud service.

***More insight on IT outsourcing
and the cloud***

To view customized survey results or read the other articles in the series, please visit www.pwc.com/itocloudstudy

