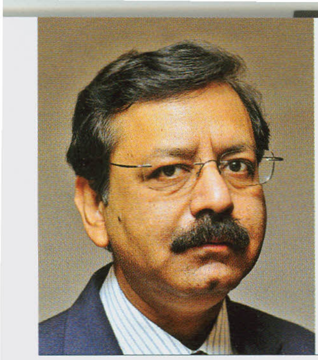

SAMEER GUPTA

Security Concerns of Cloud Computing

While cost and ease of use are two great benefits of cloud computing, there are concerns that need to be addressed when considering moving critical applications and sensitive data to public and shared cloud environments

In the world of computing the paradigm has shifted from mainframes and client server models towards cloud computing. The rest of the world has already moved towards the cloud architecture because of the inherent nature of the model. Significant advantages like bringing down the capital expenditure of any IT project and the deployment and usability of any solution are associated with cloud computing. So if this new methodology is so great why are we skeptical about getting into the cloud space?

While cost and ease of use are two great benefits of cloud computing, there are significant concerns that need to be addressed when considering moving critical applications and sensitive data to public and shared cloud environments and that includes security and bandwidth utilisation especially in Oman. To address these concerns, the organisation and the cloud provider must develop sufficient controls to provide the same or greater level of security than the organisation would have if the cloud were not used.

Listed here are ten items to review when considering cloud computing.

1 **Where's the data?** Oman as a country has different requirements and controls placed on access. Because the data would be in the cloud, we may not realise that the data must reside in a physical location. The cloud provider should agree in writing to provide the level of security required for your customers. And ideally for Oman, the service provider should have the data centre within Oman in a secured location.

2 **Who has access?** Access control is a key concern, because insider attacks are a huge risk. A potential hacker is someone who has been entrusted with approved access to the cloud. If anyone doubts this, consider that in early 2009 an insider was accused of planting a logic bomb on Fanny Mae servers that, if launched, would have caused massive damage. Anyone considering using the cloud needs to look at who is managing their data and what types of controls are applied to these individuals. This can be achieved by introducing a control mechanism like activity monitoring and data leak prevention suites.

3 **What are your regulatory requirements?** As a country, Oman has its own regulations and any organisation operating within the country would have to abide by regulatory requirements (e.g., ISO 27002, Safe Harbor, ITIL, and COBIT). The organisation must ensure that its cloud provider is able to meet these requirements and is willing to undergo certification, accreditation, and review.

4 **Do you have the right to audit?** This particular item is of no small matter; the cloud provider should agree in writing to the terms of audit. And in Oman, this can be done jointly by the organisation and an authority like ITA who could run a periodic audit on the companies who want to be cloud providers.

5 **What type of training does the provider offer their employees?** This is actually a rather important item, because people will always be the weakest link in security. Knowing how the provider trains their employees is an important item to review. Ideally the cloud service provider should have a dedicated training unit.

6 **What type of data classification system does the provider use?** Questions you should be concerned with here include: Is the data classified? How is your data separated from that of the other users? Encryption should also be discussed. Is it being used while the data is at rest and in transit? You will also want to know what type of encryption is being used. As an example, there is a big difference between WEP and WPA2.

7 **What are the service level agreement (SLA) terms?** SLA serves as a contracted level of guaranteed service between the cloud provider and the customer that specifies what level of services will be provided. The organisation should always be asking for a financially backed SLA or else it won't make any difference to the cloud provider.

8 **What is the long-term viability of the provider?** How long has the cloud provider been in business and what is their track record? If they go out of business, what happens to your data? Will your data be returned,

and if so, in what format? As an example, in 2007, online storage service MediaMax went out of business following a system administration error that deleted active customer data. The failed company left behind unhappy users and focused concerns on the reliability of cloud computing. This should be part of the audit and the concerned parties should always look into different to ensure data availability.

9 What happens if there is a security breach? If a security incident occurs, what support will you receive from the cloud provider? While many providers promote their services as being unhackable, cloud-based services are an attractive target to hackers. As a practice, the cloud service provider should run periodic vulnerability tests like penetration testing, breach testing etc. to make sure that the system is robust. And these can be done by an in-house team or a third party.

10 What is the disaster recovery/business continuity plan (DR/BCP)? While you may not know the physical location of your services, it is physically located somewhere. All physical locations face threats such as fire, storms, natural disasters, and loss of power. In case of any of these events, how will the cloud provider respond, and what guarantee of continued services are they promising? As an example, in February 2009, Nokia's Contacts on Ovi servers crashed. The last reliable backup that Nokia could recover was dated January 23rd, meaning anything synced and stored by users between January 23rd and February 9th was lost completely. In situation like this, a tier III disaster recovery architecture where there are multiple backup sites to sustain the business should ideally be in place.

11 What would be the bandwidth utilisation of the services? Any cloud service provider ideally should include the bandwidth utilisation matrix to its customers, so that the customers are aware of the load it has to take on its network. And because of the geographical architecture and high cost for network and telecommunication, the telecom ISPs could come out with some introductory plans to promote cloud computing.

Cloud computing offers real benefits to companies seeking a competitive edge in today's economy. Many more providers are moving into this area, and competition is driving the prices even lower. Attractive pricing, the ability to free up staff for other duties, and the ability to pay for "as needed" services will continue to drive more businesses to consider cloud computing. The decision to move to cloud-based services should fit into the organisation's overall corporate objectives. Before any services are moved to the cloud, the organisation's senior management should ensure such actions are consistent with their strategic plans and meet acceptance criteria that address the ten items discussed in this article.

Just as there are advantages to cloud computing, there are also several key security issues to keep in mind. One such concern is that cloud computing blurs the natural perimeter between the protected inside and the hostile outside. Security of any cloud-based service must be closely reviewed to understand what protections your information has. There is also the issue of availability. This availability could be jeopardised by a denial of service or by the service provider suffering a failure or going out of business.

The author is the executive vice president Infoline,
a leading organisation in Oman catering to Information Technology
and Outsourcing needs of the companies across all industries.