Publication: The Business Times, pg 22
Date: 05 March 2019
Headline: Silver linings and dark sides of the cloud

Silver linings and dark sides of the cloud

Using cloud-based services can save business costs and improve business flexibility, but be aware of the potential risks. **BY OUH ENG LIEH**

THE usage of cloud services has become more common in recent years. Some of the typical cloud offerings familiar to SMEs include Microsoft Office Online, Salesforce CRM, SAP Cloud, DropBox and many more.

These applications broadly classified as Software as a Service (SaaS), are made available to customers on demand via the Internet from a cloud service provider's (CSP) servers. Other types of cloud-based services are Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).

For PaaS, customers have access to the prebuilt tools on the service provider's cloud-based environment to develop and deliver their applications; while for IaaS, customers have access to the storage, networking, servers and other computing resources of the service provider's environment.

Why should SMEs use cloud-based services?

Cloud-based services give SMEs access to unlimited computing power at a marginal cost, without having to manage all the hardware, software, and networks. Cloud-based services are priced on a pay-per-use basis, where companies only pay for the IT services they consume without substantial investments in equipment, applications or IT personnel.

Cloud-based services are also scalable on demand, giving business flexibility to SMEs. For example, during peak periods when customers are looking to purchase online, the online shop can request the service provider to scale up the computing power to serve more customers quickly.

Likewise, during the non-peak period, the computing power can be reduced to save business costs. The service provider can do all the necessary configuration within minutes. In this way, SMEs can easily pay for more users or modules when the business need arises.

Cloud computing data centres are often spread out across different geographic regions, nationally or globally, and can provide resilience against regional issues and local disasters such as storms, earthquakes, or cable cuts. Operational issues such as the patching and backups can be easily automated in the cloud environment.

Given the global and competitive business environment, it is essential for SMEs to be adaptable and have business flexibility to react fast to market changes.

What are the potential risks with using cloud-based services?

A key risk to using cloud-based services is the unauthorised access and modification to customer and business data. If sensitive data are stored or processed in the cloud and are compromised due to threats such as the exploitation of the cloud software vulnerabilities, it can lead to a loss of confidentiality and integrity of the data.

As compared to non-cloud based services where the data are processed and stored within the SME's environment, there are also additional network risks when the data are transferred between the SME's environment and the cloud-based environment. Proper security measures have to be adopted to secure the processing, storage, transit and archiving of the data.

For the cloud service provider to save costs and provide a lower price to its consumers, the service provider usually seeks to enjoy economies of scale by pooling their computing resources.

This involves virtualisation of the required computing resources with the cloud-based service designed to support multiple tenants (including SMEs) at the same time. In this case, data for multiple tenants are processed and stored with the same computing resources with minimum isolation, and if these services are not properly designed, it can lead to confidentiality and integrity issues.

Different regulations and policies are applied depending on the location of the data centre hosting the cloud-based service. If your business does not allow data to be processed outside a country, choosing a cloud-based service that is physically located outside the country will lead to compliance and legal issues.

It can also be hard for customers to migrate to another cloud provider, a situation known as vendor lock-in. Vendor lock-in can become an issue when circumstances force a customer to migrate to another provider, for example in case of a legal conflict, issues about billing, major outages, etc. If the service does not provide a data export function or does not use standard data formats and interfaces, then migration may become challenging and time-consuming.

> Service providers are also likely to use other cloud-based services to provide their cloud-based service. In this case, the risks are further magnified.

Service providers are also likely to use other cloud-based services to provide their cloud-based service. In this case, the above risks are further magnified.

What are the possible actions SMEs can take to mitigate these risks?

Before procuring a cloud-based service, SMEs should have an idea about the service provider's organisational structure and their risk management processes. It is important to know how and which parts of the provider's organisation will be dealing with security incidents, how to find security-relevant information, security advisories, information about outages and the responsibilities/liabilities for security incidents.

From a software and data standpoint, SMEs can also ask questions such as how does the provider ensure software security, how customer data or processes are protected from unauthorised physical and logical access, how data can be exported and in what formats. Customers should be able to monitor the performance and security of the service, via dashboards and reports.

SMEs can also refer to the Multi-Tier Cloud Security (MTCS) Singapore Standard (SS) 584, especially for those who find it challenging to evaluate cloud service providers. MTCS standard seeks to drive cloud adoption across industries by giving clarity around the security service levels of cloud providers, while also increasing the level of accountability and transparency from cloud service providers. MTCS standard describes three possible tiers of cloud security.

In brief, Tier 1 is designed for non-business critical data and systems targeting low-impact information systems. (for example, website hosting public information); Tier 2 is designed for organisations to run critical business data and systems in a moderate impact information systems (eg, e-mail/CRM – Customer relationship management systems); Tier 3 is designed for companies with specific needs and more stringent security requirements in high-impact information systems using cloud services. Certification of the CSP is based on the type of service and carried out by accredited third-party certification bodies. SMEs can have a better gauge of a particular CSP suitability based on their required tier of security.

The writer is assistant professor at the School of Information Systems, Singapore Management University