Silver or black lining?

The security of Cloud services

Services offered by cloud providers have been in high demand in recent years. Giant companies like AWS, Microsoft and Google are topping the list of cloud service providers, and it is expected that the demand for these services will continue to grow to over US$400 billion by 2020. Yet despite their multiple benefits, cloud services may contain a black, rather than a silver lining. Now is the time for organizations to obtain a better understanding of the benefits and risks associated with the adoption of cloud services to make an informed decision before making the leap.
What is the Cloud?

Cloud computing, in its simplest definition, is nothing but a pool of servers with high processing power connected together, through highly available networks, to provide end users (consumers) with specific services such as storage, email, and enterprise resource planning systems (ERP), to name a few.

The concept of sharing computing and infrastructure resources results in reducing the cost for the consumer and capitalizing revenue for the provider. The diagram below shows a simplified illustration of cloud infrastructure.

Worldwide public Cloud services revenue forecast (billions of U.S. Dollars)

Source: Gartner

Simple illustration of Cloud infrastructure

Security practitioners are concerned with data privacy and security, ITO practitioners are interested in operational efficiency, and CEOs and CFOs promote cost savings. So how can these key stakeholders meet half-way?
The adoption of Cloud services is a hot topic in the C-suite. It recently got the attention of the global markets due to the flexibility, high availability and wide range of services it offers, its cost efficiency (arguably) and reduced operational overheads.

The services offered by Cloud providers are expected to have an increased demand in the upcoming period. An article published by research and advisory firm Gartner expects cloud adoptions to influence more than 50 percent ITO (IT Operation) deals by 2020.1

The future of the Cloud in light of the security threat landscape

So what is the future of the Cloud? Does the Cloud provider secure our most valuable assets (our data) as we expect it to? What are the security concerns we need to be aware of when adopting Cloud services? How do we utilize Cloud services without enlarging the data and security threat landscape?

Security practitioners are concerned with data privacy and security, ITO practitioners are interested in operational efficiency, and CEOs and CFOs promote cost savings. So how can these key stakeholders meet half-way?

Cloud adoption advantages

Cloud services have enriched the technology landscape with many advantages, we are highlighting the most appealing ones below:

1. Cost effectiveness (pay only for the service you use)

One of the main reasons most businesses prefer Cloud services is the reduced cost.

Cloud services offer a very cost-effective solution to manage and maintain the IT infrastructure, they also reduce the effort and operational risks associated with information technology while maintaining a very good level of service.

Adopting Cloud services may seem to be the right decision for any business owner due to the benefits it offers. The question is: “What is the flip side?”

Cloud security concerns

1. Data privacy and security

67% of Cloud services do not specify that the customer owns the data in their terms of service2

89% of Cloud services do not support encryption of data at rest2

Any discussion involving data must address data privacy and security.

Before organizations store (or process) their data by any third party (including Cloud providers), they must think about how this third party will treat their data.

For some countries, governments are very conservative when it comes to hosting their data on the Cloud. Governmental data laws (similar to those in Saudi Arabia) started to regulate hosting data on the Cloud and mandated that any governmental critical data needs to be hosted within the country’s geographical boundaries.

Controls such as how the data will be stored, how it will be encrypted, who will have the encryption key, who will be able to read and/or modify the data, and what are the governing privacy laws imposed on the data centers hosting the data.
should be addressed and cleared before such a decision is taken.

2. Loss of control over your data

40% of Cloud services replicate data in geographically dispersed data centers.

When organizations move their data to the Cloud, they are trusting, and heavily depending on, third party infrastructure. They would not maintain the same level of control they had on their backend infrastructure. One of the main elements where the organizations do not have control is the specific location where their data will be stored.

Questions about the financial stability of the Cloud provider, the geopolitical impact, political value of the data, impact of local regulations in the hosting country, geographical threats, etc. need to be addressed and clarified when taking a decision to move to the Cloud.

3. High dependency on the internet

If you experience outage in your internet connection, your business is down. Good Cloud providers may still have their business continuity plans but they cannot guarantee the continuity of your business without you being able to reach them through your own internet connection.

For organizations to maintain secure cloud services implementation, they need to understand the importance of addressing the security risks associated with Cloud implementations through baselining the Cloud risk assessment on single (or multiple) standards that are designed for Cloud security.

For organizations to maintain secure cloud services implementation, they need to understand the importance of addressing the security risks associated with Cloud implementations through baselining the Cloud risk assessment on single (or multiple) standards that are designed for Cloud security.

Cloud risk assessment

The very initial step in any new service adoption is to understand the service and all the elements associated with it. The way to do that is by performing a risk assessment.

In this article, we will highlight one risk assessment approach that should be followed when adopting Cloud services. We will base the example on Microsoft Office 365, one of the most common cloud adoptions.

Step 1: Identify threats and inherent risks

The first step in the risk assessment process is the identification of threats and inherent associated risks following the standard risk assessment practices. This step would include assets identification as well as identification of insider, outsider and external threats, and prioritize them considering the number of threat actors and attributes.

Step 2: Product risk assessment

The second step is to perform specific Microsoft Office 365 product risk assessment. This step would highlight any security and privacy issues (or
challenges) with specific Office 365 product implementation (e.g. Outlook, OneDrive, SharePoint online, etc.) along with a Go/No-Go assessment that would contain specific questions about each product to assist in deciding whether adoption of any Office 365 products would be aligned with the organization’s overall business strategy.

**Step 3: Develop security model**
Finally, a security model should be developed to identify the security controls in alignment with the defined framework. The model would be used as a guideline for defining the cloud security controls that are required before implementation of the services. The framework can be defined using single or multiple standard frameworks.

**Conclusion**
Despite the benefits that adoption of Cloud services can offer (cost effectiveness, reliability, or flexibility), organizations need to be aware of the associated risks and work on mitigating, or reducing them to an acceptable level commensurate with the overall risk appetite of the organization.

by Tamer Charife, Partner, Risk Advisory, and Mohamed El Nems, Manager, Risk Advisory, Deloitte Middle East

---

**Endnotes**

The very initial step in any new service adoption is to understand the service and all the elements associated with it. The way to do that is by performing a risk assessment.