Media title: How to avoid cloud risks
Author: Robert Trong Tran - Director, Cyber Security Assurance Service PwC Vietnam
Source: Vietnam Investment Review dated 02 April 2018
Online link: http://www.vir.com.vn/how-to-avoid-cloud-risks-57879.html

How to avoid cloud risks

A recent series of high-profile breaches and leaks of sensitive data all over the world – such as with Dropbox, Tesla, and Yahoo! – have shined a bright spotlight on cloud security and forced many companies to re-evaluate their cloud readiness, architecture, and security. **Robert Trong Tran**, director of Cyber Security Assurance Service at PwC, talks to *VIR* about how to avoid cloud security pitfalls.

Potential cloud threats

In Vietnam, the importance of cloud security has often been underestimated. Many business leaders still consider cloud services as the best solution for ensuring data security. This is not entirely accurate.

The aforementioned incidents had several things in common. All occurred on a public cloud, where security configurations are sometimes complex, disjointed from on-premises standards, and often misunderstood.

All companies could have benefited from a more detailed design and implementation of cloud infrastructure, business processes and security policies, and all suffered from a vaguely defined 'shared responsibility model' that created exploitable loopholes.

It doesn't end there. In the broader market, there are many common pitfalls which are often left unaddressed. According to the Lloyd's Class of Business guidance report "Counting the cost: cyber exposure decoded", an average loss from a serious cloud service disruption could cost the global economy as much as $121.4 billion.

With proper architecture, governance, monitoring, and cyber hygiene, organisations can better prevent future cloud data leaks – and create a competitive advantage in the marketplace through increased trust.

Avoiding cloud security pitfalls

According to PwC's studies, six common pitfalls are encountered by many businesses who undergo the transformation from on-premises to cloud. These include limitation in visibility to data and applications access; lack of policies and standards set for configuring cloud infrastructure; lagging governance to support the rapidly growing cloud landscape; the undefined 'shared responsibility model'; siloed security operations in a hybrid environment; and the inability to control human errors.

Some companies have *limited visibility into what applications are running in their cloud*, what data they have there, and who has access to the data and applications. This is further complicated by the fact that for most organisations, 'cloud' really means many different cloud providers.

There are existing technical solutions, like utilising a cloud access security broker (CASB) that can help increase your visibility into cloud activities. Companies can track who did what, from where, and when it happened.

Companies should consider gaining a greater understanding of their cloud environment through the use of a cloud discovery tool; apply continuous monitoring and automation to discover the provisioning and de-provisioning of cloud resources; and locate where key assets are in the cloud, and identify potential legal, compliance, and privacy requirements..

Most companies *do not have policies and standards set for configuring cloud infrastructure*. Poorly configured systems can allow hackers to exploit vulnerabilities and lead to malicious intrusion. Organisations should define standards for configuring existing and new cloud services. They should include robust security practices in the template to strengthen cloud services by design. They should then track industry-leading practices and the latest trends, updating the template as necessary.

Business processes, policies and standards are yet to be designed that support the rapidly growing cloud landscape, taking into consideration the myriad of industry and data privacy requirements, among others. The European Union's General Data Protection Regulation (GDPR), for example, introduces many new and significant requirements such as the 72-hour breach notification. Various data privacy regulations also require data localisation or restrict data transfer to certain jurisdictions.

Security and its operating model should grow at the speed of business. Companies should implement a strategic, enterprise-wide approach to overseeing, managing and securing vital data and how to do so in a multi-cloud environment.

In many cases, *the shared responsibility model is not defined* between companies and partners in their cloud ecosystems, causing loopholes in business processes that eventually lead to security incidents in the cloud. Companies should develop a shared responsibility model with their vendors and actively acknowledge that security is a collaborative effort.

Cloud security still lags compared to traditional on-premises capabilities. Companies should extend their on-premises security capabilities to the cloud and build upon those capabilities. Companies should also correlate on-premises and cloud incidents to help ensure threats are identified before they spread across environments.

The above issues are further compounded by *the lack of security processes, automation in the cloud and cloud development operations (DevOps)*, creating an environment in which more human errors can occur. Companies should automate the deployment and operations aspects of the cloud, especially DevOps, by automating core security tasks, including: secure orchestration and provisioning, vulnerability management, patch management, continuous integration and deployment, the security helpdesk, and security metrics generation and reporting.

Long-term strategies required

Companies should have a cloud architecture that is designed with security in mind. Robust processes focused on protecting data loss are also vital.

Companies should consistently review their cloud architecture and supporting cyber security programs and protocols, and diagnose potential problems before they occur. Proactively establishing and implementing industry-leading architecture principles and standards, technology design patterns, and accompanying operational processes is key.

Strong data and access governance is essential for thriving in the digital economy. Leadership should allocate adequate time and resources to truly address cloud security, and ensure it is a priority as part of the overall transformation to cloud. This requires board-level buy-in and responsibilities distributed throughout the enterprise. Companies should realise the cloud is unique, a place where distributed data dictates a new way of thinking about security. Increased visibility – knowing where your data is, and who has access to it – is critical.

When combined with the principles outlined above, automation can greatly reduce the risk of human error while keeping pace with the velocity and elasticity of the cloud. With these steps, organisations can not only improve their cloud security, but help create a more resilient data system that can create competitive advantages in an increasingly digital world.■

Vu Thi Thu Nguyet, Marketing & Communications Manager, Tel: +84 24 3946 2246, Ext: 4690, Email: vu.thi.thu.nguyet@vn.pwc.com