Why the cloud may be the safest place for storing sensitive data

Transparent security needed from telecom operators to become the local trusted cloud provider

Cloud computing has been adopted by virtually all sectors of our economy, but despite this widespread dissemination, concerns about data security and privacy have always been ubiquitous among business executives. However, continuous investments in cybersecurity by cloud services providers could very well have transformed the cloud into the safest place to store data. The question stands whether telecommunications operators are keeping pace in their ambition to become the local trusted cloud provider.

Businesses today operate in a complex 'business ecosystem' where suppliers, customers, business partners and service providers closely interact and collaborate. As a result, players in this ecosystem are increasingly connected and dependent on (shared) digital business processes. These developments lead up to the necessary storage of data beyond the confines of a company. No less than 55 per cent of organisations that were interviewed as part of PwC's Global State of Information Security Survey 2015 indicate that they use cloud computing. This was a mere 38 per cent only two years before. While the benefits of cloud services – lower costs, greater operating efficiencies, and immediate scalability, to name a few – have fuelled adoption in recent years, it seems evident that a new driver is at work. Perceptions are shifting, as major cloud services vendors have continued to develop and implement increasingly sophisticated security capabilities.

Cloud computing as new revenue generator for telcos

The shifting information and communications technology (ICT) landscape has placed greater revenue and profitability pressure on telecommunications operators (telcos) than ever before. Technology vendors are cannibalising telco revenues with over-the-top offerings, and forging customer relationships with value added services. More than ever before, telcos are challenged with the need to evolve beyond network connectivity and provide distinctive service offerings – into the rapidly growing technology services market. Fortunately, telcos are well positioned to offer a number of cloud services, such as becoming cloud brokers by aggregating services, platform enablers by providing an ecosystem to leverage telco assets, enterprise enablers by optimising secure networks, and business enablers by providing industry-ready solutions across the value chain. Telcos are also ideally positioned with their distribution networks, retail stores, customer care relationships, billing capabilities, and partnerships to develop an ecosystem that simplifies the selection, management, and optimisation of cloud services to business customers.

What are the benefits of offering cloud services?

Cloud computing not just offers tremendous benefits for users, but also for the providers of cloud services. Leading motives for telecom providers to offer cloud services include:

- Virtualisation and multi-tenancy capability offer optimal capacity utilisation and high economies of scale for pricing.
- The extensive standardisation enables homogeneous and cost-effective IT infrastructure management and creates various synergies.
- Because the processes are largely automated, cloud services can be offered at greater cost-efficiency.
- A combination and integration of several cloud services allows greater potential for innovative business models.
- The internet focus and availability of services on mobile devices opens new consumption channels.
- Because IT resources are used only as needed and by many customers simultaneously, power consumption can be reduced.

Sound cybersecurity in the cloud is in the telco's own interest

An increasing reliance on digital resources involves security risks and privacy issues. Unfortunately many users of cloud services fail to implement a necessary security strategy for cloud computing before entrusting their data to a cloud provider. Yet, it is the telco's responsibility to implement the appropriate cybersecurity controls in its cloud offering. Moreover, it is in the provider's self-interest to do so.

The code-hosting and software collaboration platform Code Spaces[1], for instance, showed the world that an attack by hackers can lead to the total downfall of a successful provider. The reputation of Code Spaces was in ruins after the attack and the company was not financially feasible to resolve the security leak and compensate clients for the damage caused by the cyberattack.

'More than ever before, telcos are challenged with the need to evolve beyond network connectivity and provide distinctive service offerings – into the rapidly growing technology services market.'

The downfall of Code Spaces demonstrates that cybersecurity is of vital importance for cloud service providers. This is why they should take into careful consideration the exact compliance and security requirements of cloud users, as well as the optimal way to guarantee data protection in case of transnational data storage. Telcos need to have a sound security policy with regard to managing data migration, archiving and re-transfer of customer data, and the availability and performance of business critical applications must be ensured. On a positive note, despite a recent uptick in attacks on cloud service providers, it's important to note that these incidents did not result in reported breaches of sensitive data.

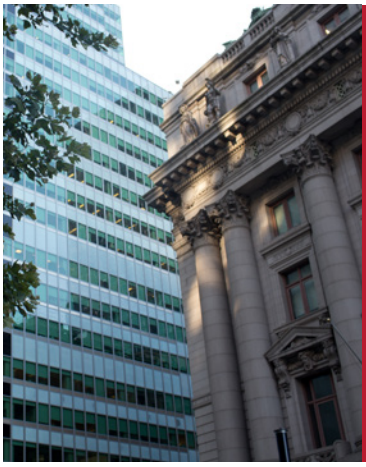
Transparency about security, as well as a definite idea about all legal and privacy-related issues arising from the underlying practices and business models are of crucial importance and should be addressed before a telco starts offering cloud services.

Generic cloud providers continue investing in state-of-the-art cloud security

Yet, when it comes to cybersecurity, leading (non-telco) cloud providers made tremendous progress in the past years due to heavy investments in sophisticated security capabilities. The implementation of the appropriate technology and processes, as well as the allocation of manpower make sure incidents can be quickly detected and mitigated.

Security measures contributed to a safe environment for the storage of sensitive data. As a result of increased cybersecurity cloud providers have obtained certifications and assessments to build trust in their security capabilities. These include ISO 27001, ISO 27018 (NEW), ISAE3402, SOC 2, PCI Data Security Standard (PCI DSS) and the European Privacy Seal (expected).

[1] http://www.networkcomputing.com/cloud-infrastructure/code-spaces-a-lesson-in-cloud-backup/a/d-id/1279116



What points should be clarified by telcos before offering cloud services?

Despite their high awareness of the topic and their technical sophistication, providers also have to answer several questions:

- What compliance and security requirements on the part of users should providers meet?
- How is data protection guaranteed in the case of transnational data storage?
- How can pay-per-use and short contractual periods be reconciled with professional services for companies without service level agreements?
- How are data migration, archiving and re-transfer of customer data managed?
- How are the availability and performance of business critical applications ensured?
- What are the legal and tax-related issues arising from the underlying practices and business models?

Transparent security measures as a unique selling proposition for telco cloud

As an example: one of the major European telcos shows that being transparent about security measures can be a way to differentiate cloud services in the market. This clears the way for cloud security to become a unique selling proposition. The far-reaching surveillance powers of the U.S. government resulting from the U.S. Patriot Act induced this telco to promote their cloud-computing services as a secure way for local and other European organisations to store classified business information. Their pitch: storing data in the cloud that cannot be accessed by monitoring foreign government institutions will attract customers who expressly wish to protect their confidential and competition-sensitive business data.

The telco as local trusted cloud provider: transparent security

Investments in cybersecurity and data privacy appear to be fruitful as more and more businesses are storing confidential information and software in the cloud. The use of cloud computing is officially mainstream across most industries. However for many business executives, potential threats to data security and privacy have always been the dark, untrustworthy side of the cloud. It's a long-held belief – and one that's starting to change. High level and transparent security: here lies the opportunity for telcos as local trusted cloud provider.

The security capabilities leading (non-telco) cloud providers implemented to ensure data protection and network security include: firewalls, intrusion-detection systems, and denial of service solutions. The use of, for instance, software-defined perimeters create a secure platform that can be adapted in order to deal with the techniques, tactics and procedures that are used by hackers.

In case hackers do get access to the network of a cloud provider, providers increasingly utilize the possibilities of new system development methods (e.g. DevOps) in combination with communal learning and rapid-response forensics tools to reduce the time between detection of unauthorised access and actually resolving the consequences of a hack.

As for the necessary identity and access management the staff of cloud providers should only have restricted access to customer data and those who have access to specific data should be continuously monitored. In addition, cloud providers need to have a scenario in place in case employees are either negligent or have malicious intentions.

To have a deeper conversation about this subject, please contact:

Bram van Tiel
Senior Manager -
Technology and Security
E-mail: bram.van.tiel@nl.pwc.com
T: +31 (0)88 792 53 88

© 2015 PricewaterhouseCoopers B.V. (KvK 34180289). All rights reserved. PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.