

DSA 
SPOTLIGHT
ON **CLOUD**

Supported by



Content

Five Common but Critical Mistakes in Cloud Computing	1
Hybrid Cloud - The What and The Why	2
Data Security and Sovereignty	4
Business Continuity and Cloud: A Match Made in Heaven	6
The Four Fears of Cloud Adoption	8
SingTel's Vision for Cloud	10

Note from the editor

DSA is **very pleased to have had the opportunity to work with SingTel** to create "Spotlight on Cloud".

In some respects, adoption of cloud especially SaaS is already wide spread. However the true promise of cloud computing is only in its infancy. In our opinion IT departments are starting to understand that Hybrid Cloud, Infrastructure-as-a-Service and Virtual Private Cloud is where the real promise lies.

The Data Centre itself will become increasingly virtualised and software defined. It will no longer be subject to the constraints imposed by on-premise facilities. Flexible and elastic cloud based resources will become an integrated and managed part of every data centre.

SingTel is the one of the region's leading providers of cloud hosting facilities, services and connectivity hence our desire to collaborate with them to produce this spotlight on cloud. The expertise that SingTel has provided to us as we wrote this spotlight has proved invaluable. As a result, we feel sure that this spotlight on cloud will help clarify the major issues that need to be considered as you develop your own truly integrated cloud strategy.

Allan Guiam

Editor, Data&Storage Asean

Five Common but Critical Mistakes in Cloud Computing

It is common knowledge within the IT user community that business pressures of profitability have pushed their way into IT to the point where some IT organisations are forced to turn a blind eye on established IT best practices to comply with business unit demands for faster time to market. One such case is cloud computing. Businesses see cloud computing as a way to reduce cost and offload some of the IT responsibilities to a third party.

But in the rush to adopt cloud computing, many organisations are ignoring some of the most prized learnings of information technology lore. Some may argue that “it is no longer their responsibility given IT is being outsourced to a service provider”.

This approach leads organisations to new vulnerabilities that go way beyond data security for which IT is the recognised custodian. Below are five mistakes we’ve observed and culled from discussions with users, vendors and expert consultants.

Verify Guru Credentials: We are seeing a proliferation of cloud experts in the market - many claiming to have years of experience in cloud computing and familiar with the intricacies associated with heterogeneous technology interconnects, SLA policy development and enforcement, etc. There is a growing list of organisations today that offer cloud certification. It would be prudent to check out the credentials of anyone coming to you with a cloud claim.

Review Compliance Rules for Cloud Computing:

These days, almost any business is bound by law to comply with rules related to data protection, privacy, data sovereignty and the “safe keeping” of accounting records. Some industries like banking, finance and healthcare follow even more stringent compliance rules. Guess what? These rules apply to the cloud as well. This area is complex. In terms of data sovereignty, it is important you take time to understand the legislation and regulations that apply to your data then ensure that your choice of cloud provider will not breach these rules. Remember, you still remain liable if they do.

Each region also adheres to different internationally recognised standards, in areas like security some of the ISO standards are excellent benchmarks, it makes sense to check what standards your chosen cloud provider meets.

Avoid Myopic Cloud Strategy: Cloud computing is the result of the intersection and application of dozens of technologies and concepts. Its complexity is being masked by oversimplified definitions designed to appeal to the business professional who doesn’t understand nor care for the risks and rewards of cloud computing. The result is potentially a myopic cloud strategy that will fail at every new difficulty the organisation meets. Begin with an understanding of the business needs, do an inventory of currently deployed technologies, map these against the business goals, identify what cloud-based approaches may be right for your organisation, and seek expert advice.

Know and Enforce Your SLA Goals: Successful organisations have in place Service Level Agreements (SLAs) to ensure business runs smoothly. Staff are trained and certified to ensure they do their jobs accurately. Moving to the cloud does not diminish the importance of SLAs nor can in-house IT wash its hands of responsibility. One legal expert cautioned: SLA contracts for cloud computing are far more complex than those used by in-house IT organisations. Cloud SLAs are not the same as SLAs used in outsourcing either. We also highly recommend that you scrutinise your cloud service provider’s SLA commitments to you to make sure that you get the service that you expect.

Keep Your Eyes on Your Data in the Cloud: According to IDC, we live in a digital universe where data is growing at 40 percent a year and that by 2020 we will have amassed 44 zettabytes, or 44 trillion gigabytes¹. When you have that much data sitting in the cloud, be mindful of who has access to it at all times. The same rules for access to data on-premise apply in the cloud as well. So review your policies and process related to employee access to data and make sure these are applied to in the cloud.

One of the benefits that the cloud ecosystem promises is the availability of choice and the ability to move from one provider to the next. And here is where some might throw caution in the air. Once you have copied over your data to the new provider, how do you know that your old service provider has properly destroyed your data stored in their data centre? It is only prudent to make sure the outgoing service provider truly has destroyed your data.

Cloud computing is a journey not for the faint of heart and the risks and rewards are great. The above are basic stuff that all organisations – big and small – should look into to protect themselves as they dive into the cloud. Caveat Emptor! “Let the buyer beware” applies just as much to the acquisition of cloud services as it does to real estate. So please pay attention.

¹EMC Digital Universe Study with Research and Analysis by IDC, 2014



Hybrid Cloud - The What and The Why

Gartner's 2014 "Hype Cycle for emerging technologies"² lists Hybrid Cloud as being close to the "trough of disillusionment" and less than two years away from "Plateau". What does this mean in plain English? Essentially that the hype about Hybrid Cloud is over and people are about to start rolling up their sleeves to implement hybrid cloud technology. According to recent report by Tech Pro Research³, 70% of companies globally are currently using or evaluating a hybrid cloud.



We spoke to **Heng Wai Mun, Head of Hosting and Cloud Services at SingTel**, who said that hybrid cloud is going to be a vital component of almost every data centre. He explained that even though the momentum towards hybrid cloud adoption is gathering pace, they still come across far too many IT professionals looking for answers to a couple of basic questions:

**What is a Hybrid Cloud?
Why will I need a Hybrid Cloud?**

Definition

The "Whats.com" definition - A hybrid cloud is a cloud computing environment in which an organisation provides and manages some resources in-house and has others provided externally.

The "Wikipedia" definition - Hybrid cloud is a composition of two or more clouds (private, community or public) that remain distinct entities but are bound together, offering the benefits of multiple deployment models.

The Devil is in the Details

These macro definitions often confuse more than clarify people's understanding of what hybrid cloud is and should be.

SingTel cautioned that having a combination of public and private does not mean you have a hybrid cloud immediately.

The "magic sauce" according to Mr. Heng is the connection between the two. "The connection can be achieved in various ways but typically it will be via VPN and it is critical that the network management is abstracted from the networking hardware". He explains further: "Enabling orchestration across this connection is the other big differentiator". Orchestration is the ability to run and load balance computing processes and workload across all components of your hybrid cloud. Successful orchestration depends on true interoperability between your on-premise IT and your cloud environment to ensure a seamless experience across these different environments. Any serious cloud provider must provide you with orchestration management via portal access. According to Mr. Heng, this is an area that SingTel has built world-class capability.

Two additional aspects of cloud computing – whether public, private or hybrid – are portability and interoperability. Data may need to move between applications, systems and platforms. This portability requires that the underlying systems, including servers, storage and networks are able to interoperate. These two requirements further introduce complexity in what IT is already expected to manage - in-house, private, public or hybrid.

"The key is to have the correct level of networking skills to create the connection as you need it. Once the connection is in place between your public and private cloud allowing for flexible movement and sharing of data and compute resources between the two, only then, in our opinion, do you have a hybrid cloud," he continues.

Why you need a Hybrid Cloud

Having clarified what hybrid cloud is, the next logical question is, "why does it even matter?".

A hybrid cloud solution offers a number of distinct advantages for organisations undecided on the technology path to take. A hybrid approach allows an organisation to experience the cloud without a wholesale exit from an organisation's existing IT strategy. Let's face it, most enterprises have invested in infrastructure over periods of years and migrating wholesale is neither practical nor risk free.



Hybrid cloud allows an organisation to realise the benefits of flexibility and scalability of the cloud while containing the risks and ensuring compliance. With a hybrid approach, an organisation can keep its data local to meet sovereignty or other regulatory compliance issues, including data security, without sacrificing on the ability to draw on resources when need to.

Many businesses must follow cycles of peaks and downturns. A hybrid approach gives them the ability to draw upon the additional computing resources for peak workloads and scale back down when business is quiet.



Conclusion

If the transformation of multinational IT vendors into cloud-oriented companies is any indicator, we are witnessing a seismic shift in corporate IT today.

Mr. Heng highlighted some tangible examples of how SingTel is assisting customers in their move to the cloud.

Backup and Disaster Recovery (DR). For backup, hybrid offers a readymade solution with primary data residing on private cloud being backed up to a more cost effective scalable storage on public cloud. When it comes to DR and Business Continuity (BC), hybrid is arguably a revolutionary approach. For instance, SingTel Cloud removes the need for n+1 redundancy and enables immediate failover to public cloud in the event of disruption in the private cloud. Hybrid allows companies that previously could not entertain the cost and complexity of building a DR infrastructure to do so.

Development and Testing. SingTel explains that the benefits gained from using hybrid cloud for development and test environments are simply huge. Test environments can be

easily and quickly set up when required. When testing is complete, the task of moving back to production is as simple as making a clone and booting back in the private cloud. Testing workload no longer competes with resources allocated for production. Scale and Load can be tested more easily simply by increasing or decreasing the resources allocated to the cloud based test machine.

In addition, SingTel cloud supports the thousands of applications and dozens of operating systems so you can run your existing applications in the cloud with no changes required from your private cloud.

Cloud Bursting. This is the key benefit of hybrid cloud – leveraging public cloud for peak and unexpected usage, and thereby enabling capital investments in hardware to be sized based on average workloads rather than peak load. This avoids over-capacity situations typically found in traditional on-premise approach to data centre build-out.

Interestingly SingTel points out that when it embarks on a hybrid cloud planning project with a new client, part of the process is to study current average and peak usage. Very often IT managers are shocked to see just how under-utilised their compute capacity actually is. Mr. Heng also pointed out that the unquantifiable benefit of cloud bursting is the unforeseen spin offs, including new projects, POCs and tests, that you can now run because it's so easy to create the compute resource and place it in the public cloud where it will not



compete for resource with your live applications.

SingTel Managed Cloud is designed to solve real IT challenges. For example, being able to separate a single workload between private and public and only moving the non-sensitive elements into the public cloud. Also, SingTel built its services to ensure that “out-of-the-box” is able to support thousands of applications and dozens of operating systems so that migration to the SingTel cloud is a pain free and simple process.

The key takeaway here is that your choice of partner on which to build your hybrid cloud is possibly a more important choice than who your public cloud provider might be. The one most critical consideration is getting your network topology right, the connection between your public and private cloud is critical. It's not about bandwidth. The configuration and management layer is the real “jewel in the crown”. This determines what you can share and move between your private and public set ups. In that respect, SingTel's credibility in understanding the “connection” is arguably second to none.

²Source: Gartner Hype Cycles 2014

³Hybrid Cloud: Benefits, roadblocks, favored vendor, Tech Pro Research's May 2014 survey

Data Security and Sovereignty

When it comes to placing your data in the cloud, security and sovereignty are two important and closely linked considerations that must be part of your thought process.

Analyst reports consistently rate security as the number one barrier to cloud adoption. The RightScale 2014 State of the Cloud Report clearly demonstrates this, with numerous similar findings from organisations like Gartner, IDC and Everest Group. Our own experience at SingTel confirms that most IT professionals tend to be far more pre-occupied with security than they are with sovereignty.

The reality is that where most people are concerned with security perhaps they should also be concerned about data sovereignty.

Whilst data security challenges may differ with cloud technology, the issues remain the same (access control and privacy). However, the effect of cloud on data sovereignty is a game changer for many organisations and the implications can be much more serious, particularly with heavily regulated industries or organisations with a global footprint.

IT takes the brunt of responsibility for moving the organisation's IT infrastructure to the cloud, security issues on- or off-premise remains one of the highest priorities, and biggest risks, for the IT organisation charged with being the custodian of the company's most important asset – information.

For most IT professionals, sovereignty is a legal and regulatory issue and hence, it is not always at the forefront of IT concerns.



So what is data sovereignty? Why does cloud have such an impact on this issue?

Put simply, data sovereignty is about who has legal rights over your data. When you spend a minute to think about this, it is clear that cloud has changed issues, considerations and laws around data sovereignty.

Consider these points:

Data held in the cloud may be subject to the laws of more than one nation.

The legal onus is on you, not your cloud provider to comply with local laws.

Different data (for example, health records, HR data, transactional data, etc.) are subject to different laws in different locations.

Companies storing data in the cloud are subject to the laws of the nation hosting the data and the laws of the country in which the business is incorporated. The result is a possible dangerous conflict around data sovereignty laws.

The difference in the local legislation and rules around data sovereignty across Asia, never mind the rest of the world, is huge. Laws regarding who has right to access or audit data, what type of data can be shared, the legal process for gaining access or warrants to view the data, and censorship and liability laws differ from country to country.

One of the most comprehensive studies on this subject in Asia was the **2013 Data Sovereignty Report** conducted by the **Asia Cloud Computing Association (ACCA)**, which makes for interesting reading for anyone who needs to delve deeper into this issue.



One of the most important factors highlighted in the report is what ACCA termed 'Regulatory Stability and Enforcement'. This is an assessment of how clear and simple it is to do business and how fair and effective laws and regulations are enforced. Singapore is rated top of the list in this respect. On further examination Singapore's total approach to data sovereignty is transparent, fair, well regulated yet open enough to allow the flexibility that cloud-based business needs*.

Whilst cloud does not impact security so fundamentally as it does sovereignty, the two issues are joined at the hip especially when it comes to the privacy of data. In reality the technical security challenges presented by cloud are not a great leap from the security solutions put in place for a typical corporate network. The same issues and technologies come into play.

In our experience, many enterprise security fears are rooted in the lack of understanding (a.k.a. distrust in what people are not familiar with) of the shared infrastructure multi-tenancy setup of public cloud. Understandably, how easy is it for a business

person to visualise the concept that cloud computing is built on a software abstraction layer? This means that the security and protection of your data is no longer at a hardware level; that it has to be achieved through software. What most people don't know, however, is that this is a reality present in most data centres today, and not exclusive to cloud computing.

The reality is that reputable and experienced cloud service providers will likely have more resource and in-house experts with security capability than almost any typical enterprise IT department. What this means is that when you work with a serious cloud player, the considerations they have already given to security means that your hosted infrastructure is very likely more secure than your own IT operations.

What you need to be aware though is that **when it comes to security all clouds are not created equal.**

To feel secure in the cloud, your peace of mind can only be achieved by checking your service provider's capability and credibility in this domain. Beyond that it is still down to you to create and enforce your own security policies. You would do well to remember that most security breaches still come from people within your organisation. Things like lapsed password management and policies still exists in the cloud, as they do in your own data centre.



Both security and sovereignty should be high on your list of considerations when choosing a cloud service partner on which to build your cloud infrastructure - public, private or hybrid. Sovereignty, in our opinion, is the trickier of the two. We believe we are well positioned to help companies from across the whole region navigate these two important issues.

** SingTel strictly adheres to Singapore Data Sovereignty legislations and regulation.*

To find out more about how we can help you with your own data sovereignty policies, email us at cloud@singtel.com.

Business Continuity and Cloud: A Match Made in Heaven

If there is one application that was specifically designed for use in the cloud, it has to be Business Continuity (BC) and Data Protection.

When people talk about business continuity in the cloud, two questions that come to mind:

1. What built-in resilience does your cloud provider have?

2. How can the cloud be part of the business continuity plans for your on-premise applications and hardware?

On the first point, reputable cloud providers have built into their infrastructure multiple levels of redundancy and resilience as standard that far exceed anything you may have in place in typical on-premise IT. As an example at SingTel, we build redundancy into every element of our infrastructure and network. In addition, our cloud users have the option to deploy their cloud across two data centres running concurrently with near real time replication between the two in an active-active configuration. This ensures a level of redundancy for your infrastructure, applications and data that is just not feasible for most corporate IT departments and is not matched by many other cloud providers.

On the second point, using the cloud to build business continuity environments is a democratisation of a discipline which used to be the preserve of companies that could quantify data loss and downtime into thousands or even millions of dollars per minute.

Cloud changes the BC game

Whether your primary systems sit in a traditional data centre, on your own private cloud or even in public cloud, the possibilities and economics of enhanced Data Protection, Disaster Recovery and Business Continuity have opened up to everyone.

Cloud, in all but a select few cases, removes the need for dedicated Disaster Recovery (DR) facilities. This alone has re-written the rules for business continuity. Anyone can spin up a recovery environment in minutes in public cloud. The need to rent or own a DR location has vanished. The need to have redundant and DR hardware sitting idly waiting for a failure has also disappeared.

At SingTel, we can offer cloud based storage and the ability to spin up cloud based compute (servers) running numerous industry standard operating systems within minutes. So what does this mean for your business continuity?

1. Backups can be directed to the cloud, meaning you can automatically have an offsite copy of your backup data.

2. Servers can be spun up in our cloud, meaning in the event of a complete disaster or hardware failure, your offsite backup can be recovered in minutes onto a Virtual Machine residing in our cloud.

3. Host-based replication software are available from many third parties which enable you to create an identical copy of your primary servers in our cloud and keep these in sync with real time replication. In the event of a disaster, a failover can be initiated in seconds and business disruption completely avoided.

To create an equivalent non-cloud based business continuity environment with the broad features above is cost prohibitive to all but a few.

Offsite backup would require services of companies who would physically come to your office, collect your tapes and store them in their own off site location. Having a standby server would require redundant hardware and rented rack space at a second location, which would sit idle and unused for the majority of its lifetime.

In today's world, there is rarely a situation where it makes sense to have redundant hardware sitting around waiting for a disaster.

Anyone that is not using cloud as an automated location for offsite backup data should be asking themselves "why not?".

Cloud technology brings secure remote copies of your server and application failover and near instant machine recovery into the hands of almost everyone. Cloud has changed the economics to the point where even small companies with limited IT budgets can build BC and DR environments that just a few years ago would have cost 6 figures and up.

If you think of the cloud for nothing else at this point in time, we would strongly advise you to look at your current data protection solutions and find out how cloud can enable you to raise it to a level that just a few years ago would have been beyond your reach.





The Four Fears of Cloud Adoption

The hype about cloud computing is such that you can be forgiven for thinking that cloud adoption is universal. The truth is somewhat different! Despite the hype and the column inches dedicated to cloud computing, we are only scratching the surface of cloud adoption.



Currently the majority of corporate cloud adoption is around Software - as - a - Service (SaaS). Things like Office 365 and Salesforce.com are prime examples of SaaS. This is to be expected, buy-in can be very cheap with implementation totally separate from the rest of corporate IT.

However, the real promise of cloud is much more than SaaS. Cloud is a transformative technology where the norm will be to move compute power and infrastructure between on-premise resources, private cloud and public cloud. However we are not there yet; with many IT managers expressing doubt and nervousness about moving their on-premise computing into the cloud.

There are basically four fears that occur most often in cloud:

Security

Security is the number one fear we hear when people express reticence to move to cloud. This is entirely understandable, and directly related to the feeling of letting go. Essentially you are placing your company's most valuable asset (its data) in the hands of an "unknown" party. In the case of public cloud, there is the added

worry that it may be on a shared physical resource. The reality is that cloud providers often have more resource and knowledge of security than the most well staffed IT departments. Even consumer grade public cloud can have stronger security than the average SME IT department. When you partner with companies like SingTel that offer enterprise-grade cloud services, many companies find that the security of their data and infrastructure is strengthened rather than compromised.

That said, the same rules still apply. As with on-premise IT, it makes sense to use the services of an external security tester. This good practice should remain in place even with the most secure cloud hosted services.

SingTel understands the importance of security and has put in place multiple tiers of security to protect or customer's data, including enterprise firewalls, malware protection, IDS / IPS, as well as isolation of VMs and networks. SingTel Managed Cloud is hosted in our secure Tier 4 data centre offering the highest levels of redundancy and resiliency. In terms of connectivity, SingTel is Asia's leading MPLS IP VPN provider, with a proven secure high speed managed network service, giving total peace of mind as you interconnect your physical, virtual or cloud based data centres. In addition, we protect against the threat of cyber attacks through our 24x7 SingTel Security Operation Centres.

Service Provider Tie-in

The economic, contractual and competitive nature of cloud services is such that tie-in is just not part of the vocabulary. It's about making your service provider part of your infrastructure strategy.

As companies look at hybrid systems, integrate mission critical applications and highly sensitive data into cloud based architectures, an element of "tie-in does materialise".

However this is not a contractual or technical tie-in that people have experienced in the past with outsourcing or proprietary systems. Rather, it is a healthy tie-in based on a deepening partnership. Knowledge of your cloud service provider, their support capability, their billing options and their functional capabilities are all learned and that learning curve is difficult to walk away from.



Spiralling Usage Bills

One of the benefits of cloud is the ability to avoid upfront capital costs and paying for compute resources on a “pay per use” model. However, be aware that there can be some nightmarish bills if you do not understand your cloud provider’s billing mechanisms.

The major problem with billing tends to be with public cloud and self-service consumption. If users do not take time to fully understand how public cloud usage and charges are calculated, you may find yourself with large wads of bills for consumption you did not even know you were making.

The reality is when done right, public cloud and hybrid cloud should make sound economic sense and bills can be predictable and well controlled.

In our experience, there are two rules of thumb to live by:

- 1. Cloud compute and infrastructure costs less even though it costs more!**
- 2. On-demand is always more efficient than forecasting.**

These rules emphasise that if you switch off your cloud services when they are not in use you will save money; and that trying to forecast required capacity for on premise IT usually means you have to buy excess capacity that you may not use for years if at all.

Losing Control

Usually a feeling or emotional response rather than a reality, moving to cloud does not mean a loss of control over what is important, namely, the IT services and applications you deliver to the business.

Rather, it is “letting go” of the underlying technology on which these services and applications run. This becomes less important and gives IT the ability to become far more aligned to the business.

This sense of “loss of control” can come from not owning the technology. It doesn’t help that cloud providers don’t typically reveal their underlying technology when they sell you a service plan. It is important to work with a trusted service provider who can provide defined performance metrics, so that you can focus on achieving business outcomes, and not worry about the technology.

For example, SingTel’s customers go through a journey where they move from a feeling of loss to one of having greater control over the applications they provide to the business. Letting go of “keeping the lights on” actually frees up time to improve quality of service to the business.

SingTel's Vision For Cloud



DSA spoke to Lee Han Kheng, Vice President of Global Products at SingTel to get his perspective on cloud today and SingTel's vision for the future of cloud. In our view, SingTel plays a pivotal role towards the adoption of cloud services in the region. Singapore has long been a technology hub for the region. This position has become even more critical with cloud. Protected from natural disaster and

with clear, open and well defined regulations, cloud providers based in Singapore will appeal to many companies and businesses across the South Asia region.



DSA - In some ways it's an obvious step for a Telco company to offer cloud services. Can you share with us why SingTel decided to enter the cloud service provider market at this period in time?

SingTel – Our move from a pure Telco to an infocomm technology (ICT) provider was neither recent nor sudden. SingTel has built an extensive portfolio of services over and above our core telco carriage products to support enterprises, including managed networks, managed security, managed mobility, unified communications, data centres and cloud.

Cloud is a natural progression for us as we possess both the infrastructure assets and also the IT capabilities (through NCS, a part of SingTel Group) to develop and implement these solutions.

There is no doubt that cloud is here to stay and businesses will increasingly use cloud in different ways. We are already seeing many enterprises realise the benefits of cloud such as faster time to market, scalability, and cost efficiency without having to manage and integrate complex IT systems themselves. We have also seen Software-as-a-Service (SaaS) adoption lead the way in cloud adoption. This is because SaaS demonstrates clearly the most obvious CAPEX to OPEX benefits of cloud. The ultimate promise of all cloud is to consume and pay for the resources you use when you need them. It is this reality that will drive ever increasing cloud adoption.

SingTel's venture into cloud was a meticulously planned strategy. Over the past few years, SingTel has developed Infrastructure-as-a-Service (IaaS), SaaS and Platform-as-a-Service (PaaS) cloud offerings. So as things stand for us today, we do not think of this business as "new"; we already think of ourselves as a complete cloud provider. Our IT capabilities, secure network infrastructure, state-of-the-art data centers, and ecosystem of technology partners mean that we can offer enterprise grade cloud solutions today.

DSA - How do you see companies adopting cloud over the next few years (e.g. IaaS, PaaS, SaaS), and what part will SingTel play in this adoption?

SingTel - We already see many small-medium businesses (SMBs) and enterprises on cloud, especially in the area of IaaS and SaaS where the cost is 100 percent OPEX-based. We do not see a slowdown in adoption; it is a compelling business model in many ways. Cloud means companies spend less time managing their resources and applications; using these as and when they need, allowing them to focus on their core business.

Moving forward, we expect to see more use of cloud computing around business continuity. Cloud can be used to back up many mission-critical applications and databases. Instead of failing over to a hot standby site that costs millions a year in maintenance and upkeep, they will simply turn on cloud services to continue business support during disasters.

DSA - We see hybrid cloud as a turning point for the industry. Traditional IT infrastructures are fusing together with cloud infrastructure. How do you see hybrid cloud affecting IT as we know it and does SingTel have a hybrid strategy?

SingTel - The days of thinking of only a private cloud or public cloud approach as separate and distinct IT strategies have already passed by. These days, a practical third option exists.

We are starting to see a lot of interest in hybrid cloud; but also a lot of confusion. Having a private cloud and a public cloud does not mean that you have a hybrid cloud. The ability to transfer workloads and resources seamlessly between the two cloud environments is what makes for a true hybrid cloud strategy.

Hybrid cloud computing allows customers to keep their mission-critical data or applications on-premise while harnessing limitless computing power and storage in the cloud. This allows businesses to enjoy the benefits of data centres without limitations.

At SingTel, we believe that no company is better positioned to deliver hybrid cloud than we are. We started by offering private cloud to enterprises, followed by offering virtual private cloud hosted at our secure data centres. It wasn't long before we started selling public cloud.

When you combine this with our roots as a telco, we are perfectly placed to provide the network connection between the multiple cloud environments. No one can doubt our capability to provide the connection; but connection without orchestration** of connected clouds still achieves very little. SingTel has already built a web-based orchestration portal to enable complete management of resources across all elements of a hybrid cloud.

**Editor's note: Orchestration is the software layer to manage compute resources between connected clouds.

DSA - Does SingTel plan to compete with the public cloud providers? Or do you have a different plan?

SingTel - We recognise that there is no one-size-fits-all cloud solution. Our aim is to help customers get on to the right cloud for their particular workloads. For some, public clouds would be a good fit; others require more secure and robust virtual private clouds or private clouds.

It is important is that we offer flexibility, choice and reliability for our users that is not limited to the type of cloud but extends to choice and flexibility in every significant area including security, network and performance. We are gearing our offering to business users that require more user control over their cloud environment and will need to adhere to strict change control policy.

At SingTel, an enterprise-grade cloud is about being able to provide the right performance, security and resilience based on the needs of specific applications or resources, virtual private and private cloud this flexibility.

We have developed our own Virtual Private Cloud to cater to enterprises that need a level of security and the ability customised to their needs. We are delivering a higher degree of stability to ensure that we meet the compliance and data sovereignty requirements now demanded in the corporate world. That is why our focus is not so much on any one type of cloud but rather on offering robust hybrid cloud solutions giving our customers flexibility in all aspects of their cloud services and the ability to manage each of these different cloud types.

DSA - Cloud is changing the dynamics of the IT market place. Competitors are seen having to work together and companies that have never competed find themselves coming head to head. Who do you see as partners and competitors in the cloud paradigm?

SingTel - We are driven by our customer's interests. As such we understand the need for healthy competition in the cloud market place to ensure that customers get the optimal cloud solution for their requirements.

As an example, we work with best of breed technology partners like Microsoft in the SingTel Managed Cloud. More than this, we recognise that some of our customers may need to place workloads on Public Clouds. To facilitate this we work with Microsoft to provide secure MPLS connections directly into Microsoft Azure. Our cloud portal is also designed to allow customers, in future, to subscribe to public clouds like Microsoft Azure or AWS. This approach resonates with customers. It enables SingTel to act as a trusted cloud advisor, who can help them understand, utilise and consume whichever cloud solution is best for their requirements.





DSA - Do you see cloud impacting work practices in Singapore and beyond in the near future?

SingTel – Yes, without a doubt. If you look at the non-IT impact of cloud on work practices, cloud brings a workplace together regardless of time and geography. Cloud will increasingly mobilise the workforce, making more people in more professions less tied to a specific office location. The impact can be immense. Just one example is how cloud might reduce travel and congestion as media rich collaboration becomes increasingly possible.

From an IT perspective cloud changes work practices hugely. Cloud abstracts the technical leaving IT people to focus on service levels. As an example, traditionally, IT teams had to seek funding for additional equipment, data centre space, and focus on building and configuring their IT environment. With cloud, IT teams can leave all that to the service provider.

This changes the game for IT departments. They no longer have to spend time administering the infrastructure; they can manage IT using SLAs based on application performance.

DSA - We hear a lot about “cloudanomics”. What’s your view on the economics of cloud? Is it a game changer for corporate IT?

SingTel - For me, the first three “laws” of cloudanomics put it very well.

- 1. Utility services cost less even though they cost more.**
- 2. On-demand trumps forecasting.**
- 3. The peak of the sum is never greater than the sum of the peaks.**

These get to the heart of how cloud changes computing economics. As cloud providers we are not paying less for the hardware we put in place, but each customer still makes savings as our costs are aggregated over resources that are shared. More importantly, cloud is about only using and paying for what you need when you need it. So you pay for and use resources on-demand with no lock in. And when it comes to the economics of IT - that is really a game changer!

DSA - For organisations that aren’t yet using cloud, what’s the first step they should take?

SingTel - Start with understanding your own needs and requirements, and then determine if cloud computing can provide the right value. In most circumstances, the business case will be there, but the risk of “doing cloud wrong” is real if you don’t spend the time to define your requirements first.

Moving to cloud should help reduce cost and increase business agility, but don’t jump onto just any cloud provider and don’t make your decision based on a simple cost per GB comparison. Find a reliable cloud provider that provides consultancy and knowledge to help you develop your cloud strategy and manage your workloads. It is possible that you will end up with needing the services of several cloud providers. Look for one cloud provider willing to be the single point of contact for all your cloud needs. Trust me. You do not need the hassle of running around managing different providers. Make sure that you fully understand every aspect of your cloud provider’s billing practices. Finally, assess whether areas such as their management portal, security, compliance and resilience match your needs.

DSA Spotlight On Cloud by



Supported by

