interxion™

NO CLOUD
IS AN ISLAND

Hybrid clouds offer new revenue opportunities

An Interxion whitepaper by Jelle Frank van der Zwet & Ian Murphy

INTRODUCTION

Business computing stands at a crossroads. There is no more tolerance for the costly, under- delivering, grand IT projects of the past. Instead, IT must evolve to be business agile, create competitive advantage and deliver on time. Most of all, IT has to not only be cost-conscious, it has to learn to be frugal, making the most of every resource.

Companies increasingly look at cloud-based technologies as a means of delivering the next generation of IT via a low cost, dynamic and flexible resource platform. However, not every application will go into the cloud. Core business-critical systems are likely to stay in-house, while less sensitive systems are ideal candidates for cloud deployment.

To make cloud and on-premise systems work together poses some significant challenges that are explored in this paper, including:

- Integration of cloud and on-premise systems
- Workload optimisation
- Application rationalisation to identify cloud-suitable systems
- Provisioning the correct level of bandwidth
- Defining and managing Service Level Agreements
- Creating new cloud services and business opportunities
- Building community and common interest clouds
- Selection of the most appropriate data centre infrastructure

To help IT meet these challenges, system integrators have a great opportunity to adapt their existing business models. Over the last two decades they have enabled customers to migrate to multi-platform delivery models incorporating, amongst others, distributed computing, web services and thin client technology.

Cloud is just another delivery platform where the key is understanding and rationalising the delivery process. This is the core competence of the system integrator – taking complex interactions and turning them into IT solutions. In this paper we will identify where system integrators can bring their experience to bear and how they can integrate cloud into their strategic solution platforms.

WHY CLOUD COMPUTING APPEALS TO YOUR CUSTOMERS?

As IT budgets continue to be squeezed, companies are looking at ways to cut their IT costs. An increasingly attractive option, Cloud computing, holds out the promise of a cost-efficient, flexible way of delivering IT to the business, by better use of resources.

Enterprise IT is a heterogeneous mix of modern and legacy platforms of many vintages. With the emergence of a variety of cloud service models (IaaS, SaaS, PaaS) and deployment models (private, public), the enterprise IT of the future will feature a mix of cloud platforms.

Cloud computing is a great fit for some applications and workloads. However, there will always be some data, processes, and applications that will remain on-premise for reasons of regulatory compliance, mission-critical or classified data, control or cost.

Large enterprise IT departments see several benefits from cloud computing. Among these is a more efficient way to manage budgets, IT maintenance and upgrade programmes. This is because cloud computing offers flexible access to IT resources, skills, new technologies and the latest updates and patches for servers, tools and applications. All this without the management, licensing and purchasing headache this would normally involve.

For smaller organisations, cloud computing levels the technology playing field. Access to resources and technologies beyond anything their usual budgets could afford enables them to take their business to the next level. Importantly, they gain access to the people and processes that can help create competitive advantage from these new technologies.

A WORLD OF MANY CLOUDS

Cloud infrastructure enables IT organisations to share computer resources across multiple applications and user groups in a dynamic way. Applications, middleware, and infrastructure are no longer tightly coupled and resource allocation is fast and flexible.

There are three key cloud models: private, public and hybrid, and market-focused versions such as community clouds that address specific markets and groups.

A private cloud is where the resources are owned and accessed only by the enterprise, whereas the public cloud is a shared environment. For some applications and organisations, there is a solid business case where core applications will be in a private cloud but some applications and functions exist in the public cloud. This is known as the hybrid cloud.

Over the next few years, we will see enterprise IT departments mix private and public cloud to create their own hybrid clouds. This removes cloud silos where certain classes of applications were moved into the public cloud and then integrated with the private cloud. The hybrid solution will require a significant amount of planning and integration.

In this paper, we explore the case for hybrid clouds. We will highlight how system integrators and service providers can address these developments as an extension of their existing business model and bring IT to the new cloud reality. Finally, we will outline the importance of choosing the right type of data centre in which to build your cloud solution.

CLOUD DEPLOYMENT MODELS

Public: The cloud infrastructure is made available to the general public or a large industry group and is owned by a third-party provider selling cloud services.	Private: A cloud infrastructure operated solely for an individual organization. It may be managed by the organization or a third party and may exist on or off premises.	Community: Several organizations share a private cloud and supports a specific community that has shared concerns (e.g. security requirements, policy, and compliancy). They can freely exchange data among themselves while keeping it secure from the outside world.	Hybrid: A composition of two or more clouds (public and private) that remain unique entities but are bound together by standardised or proprietary technology that enables data and application portability and interoperability (e.g. cloud bursting for load balancing between clouds and/or data feeds for distributed applications).
Pros: Public cloud options offer cost savings and flexibility, as well as initial speed of deployment.	Pros: Possible to achieve many of the cost and flexibility benefits of public cloud without the concerns associated with having data stored in a public environment.	Pros: In industries such as health care, government, and defence, a community cloud provides a secure channel for the seamless transfer of vital data.	Pros: Hybrid clouds can offer the flexibility and cost savings of the public cloud along with the security and data protection of the private cloud.
Cons: Business decision-makers may resist having key data off-site or away from IT's direct control, and may not trust the security of data stored on servers shared with other customers.	Cons: Initial cost savings are less than with a public cloud, but long-term cost savings will in some cases exceed that of public cloud. This requires in-house expertise that IT-staff may not possess.	Cons: It requires a great deal of coordination among the members of the cloud community, who must also all agree on a provider or central location for the cloud.	Cons: This is the most complex cloud solution to manage, and integrating the public and private clouds requires special expertise.

Source: NIST Data and Interxion analysis

WHY HYBRID?

Enterprises see both advantages and disadvantage with public cloud. On the negative side, poor or no federated security, a lack of integration with management tools, no enterprise-ready data access controls and compliance issues. The latter will be a significant concern as compliance penalties get harsher and regulators begin to crack down on bad behaviour.

ADVANTAGES AND FEATURES OF HYBRID CLOUD COMPUTING

Many cloud computing providers have recognised the issues above. Their solution is federated tools which allow security, system management and data to be managed as if they were part of the private cloud, despite being on the public cloud. These federated solutions also provide the capability to ensure that any data or applications sitting on the public cloud can remain in compliance.

The key challenges for all sizes of business are creating the private cloud and then integrating it with their chosen public cloud. Despite the new generation of federated tools, this will not be easy as there will be business logic to be written and changes to the way software is designed. This is where system integrators and top tier distributors will find a ready base of customers looking for skills and professional services.

Correctly configured, the hybrid cloud offers many benefits. Improved SLAs, the ability to scale an application out to hundreds of servers, the ability to do very specific types of computing, such as big data or application testing. However, the most important benefit of hybrid cloud is cost reduction and better fiscal management of IT. This benefit can be realised in several ways:

- Reduced capital expenditure on new hardware and software

- Reduced running costs on datacentre power and cooling

Which Products and Services are best-fit for your needs	Public Cloud Solutions	Dedicated Private Cloud	Hybrid Cloud Solutions
Need to lower Infrastructure Costs	☁☁☁	☁☁☁	☁☁☁
Rapid Scaling / Unpredictable Growth	☁☁☁	☁	☁☁
Utility Usage / Billing Model	☁☁☁	—	☁☁
Highly Available Infrastructure	☁☁	☁☁☁	☁☁☁
Industry Standard Compliance Requirements	☁	☁☁☁	☁☁☁
High Database I/O	☁	☁☁☁	☁☁

Good ☁	Better ☁☁	Best ☁☁☁

Source: Rackspace

- Higher utilisation of resources which in turn lowers the cost of providing IT

- Metering which allows application usage to be more effectively costed

- Faster and more cost-effective access to new applications through Software as a Service

- Ability to deploy new solutions more quickly

Hybrid cloud implementations

Hybrid cloud implementation breaks into two key implementation choices: non-critical applications and the test and development cloud. Non-critical applications have no commercially sensitive data and, if unavailable, do not impact the business. The test and development option allows virtual machines (VMs) to be brought online quickly and for short periods of time.

Storing data locally or in the cloud

Concerns over the location of data is not just about security and privacy, it also affects application performance. Many applications assume that the data is stored locally. When the data is not stored locally, network latency can have a significant impact on application performance. This must be considered when moving applications to the cloud.

The use of dedicated circuits and/or a Metropolitan Area Network (MAN), ensures latency is low enough to allow the separation of data and applications. Use of the public Internet and a Wide Area Network (WAN) requires applications and data to be colocated in order to remove latency issues. Network latency must be measured and monitored in order to achieve and maintain enterprise-level Service Level Agreements (SLAs).

HYBRID CLOUD ADOPTION

Enterprises will pick and choose applications and vendors based on their business needs, thus creating a diverse and heterogeneous cloud environment.

Examples of hybrid cloud adoption today are:

- **Corporate websites**. These are moving to the public cloud to improve access and reduce the risk of downtime.

- **Online web stores**. These are using the public cloud for their catalogue and transferring customers to the private cloud to complete payment options. The public cloud allows for the quick provisioning of resources when a promotion takes place. The private cloud enables the securing of customer data.

Some of the aspects of cloud infrastructure working in sync with on-premise or private environments include:

• **Federated identity and security**. A critical issue for enterprise customers wanting to avoid the problem of 'shadow IT'. Shadow IT occurs when applications and data are moved out of the IT department's control and users need alternative log-in credentials to access the data. This creates problems for data protection compliance and privacy.

• **Workload optimisation**. Used as part of the cloud migration process, it provides a baseline for establishing the resources required in the cloud and the cost of running the application. This should be a key element in negotiating an SLA with a cloud vendor.

• **'Cloud-aware software'**. Mainstream software vendors, large and small, are currently rewriting their software to make it 'cloud-aware'. In-house software must also be cloud-aware by using asynchronous messaging and supporting multi-user and multi-tenancy. This can be achieved by using the latest development tools that support cloud as a deployment platform.

• **Middleware**. This is the integration 'glue' between applications in the public cloud and the private cloud. It makes it easy for software developers to connect software on local and remote platforms.

• **Managing metering, billing and relationships with multiple cloud vendors**. Still a significant challenge but the use of federated management tools to link cloud and on-premise IT are making it easier. These have to be able to support multiple cloud providers to create a single view of all platforms to ensure effective billing.

HOW TO CONNECT CLOUDS?

There are several key tasks to be undertaken when connecting to the cloud:

1. **Preparing virtual machine instances**. The quickest way for a customer to get started in the cloud is to have pre-prepared virtual machines instances (VMI) that can be deployed via a self-service menu, with immediate start.

2. **Loading applications**. If customers want applications that are not part of the public cloud offering, they will need to install them in a VMI.

3. **Loading data**. This is probably the hardest part due to the size of the data set versus available bandwidth. If the customer cannot upload the data, there needs to be a mechanism whereby they can ship a disk or a tape which can be loaded for them.

4. **Establishing the right form of connectivity**. Workload optimisation will provide data about the bandwidth required by applications moving to the cloud. This can be used to determine if leased line or public Internet is sufficient for connectivity.

5. **Deploying federated management and log-on systems**. These will ensure that cloud is just another deployment platform from a management perspective. It will enable enterprise security and administration to be applied equally to all applications,

6. **Implementing security**. Each VMI should have firewall protection turned on and they should be managed centrally to reduce risk. Where possible, increase use of Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) to detect security risks. All data should be encrypted when in the cloud and use encrypted connections to talk to cloud-based applications.

7. **Disaster recovery**. All deployment platforms have a risk of failure. Access to other data centres and replication technology that allows customers to switch data centre in an emergency is good planning.

CLOUD BUILDING CHALLENGES

Building a cloud infrastructure requires CAPEX. Hardware, software, services, applications, licences, processes, network, connectivity - all require planning and investment. Time is a key factor: getting the planning right is important, but so is time to market. Take too long creating the perfect solution and it will be hard to get noticed and outdated. Conversely, rushing to market with an under-specified solution will cost considerable sums to correct.

Cloud service delivery requires reliable, next-generation connectivity. Reliable and seamless application and service delivery across private and public clouds requires a service-oriented architecture approach. With heterogeneous systems, a single pane of glass approach to orchestrating and metering both internal and external cloud environments is essential.

In this view of the future, the IT leaders become both broker and mediator. The challenge then is to interwork between disparate cloud-based services and internal IT, connecting service requests with the most appropriate service provider and service delivery.

The CIO or IT manager role is evolving to be a service orchestrator. Service providers are rapidly becoming mission-critical suppliers, providing truly transformative business services. A few years ago, anyone building a cloud would have to do all the heavy lift themselves. Vendors such as Citrix and Flexiant have changed this with solutions for cloud builders.

THE KNOWN CHALLENGES ARE…

Infrastructure and Virtualisation

Hardware is increasingly power-efficient but although prices have fallen, it can still be expensive. The current recession has seen significant amounts of hardware, often less than three years old, on the quality second hand market making it affordable for many businesses.

Virtualisation has improved with large vendors such as Microsoft targeting utilisation rates on commodity hardware of 60%. This will continue to improve over the next few years. Power and cooling costs are also coming down, due to better data centre design, more efficient hardware and higher input temperatures allowing a longer period of compressorless cooling.

Software and Services

Cloud is more than just virtualised servers, storage and networks; it needs software and services. The challenge is creating an automated and controlled environment with proper management and governance tools.

Vendors such as Cisco and Flexiant have solutions for cloud builders. Cisco's vBlock (with EMC and VMware) sits on top of commodity hardware, providing a service and application stack, minimising the need for specialised hardware.

Flexiant is a solution with an easy-to-understand licensing model. It provides master images that can be quickly deployed for customers. Unlike vBlock solution it does not have all the built-in links to federated security, management or workload solutions; those have to be bought, installed, configured and licensed separately.

The importance of partners

The major hardware and software vendors are building out their own cloud environments, and looking to sell their products to other cloud providers. Choosing the right partner is important because they will have lease programmes for hardware and software and will work with you on resolving issues such as software licensing.

Secure by design

Building a new cloud is an opportunity to invest in the right level of security. Too often, software is seen as being insecure by design, demonstrated by the constant patching of products. A cloud development is more complex than a single client solution. You may be sharing hardware and even services across multiple clients, so there is a need to ensure the physical and logical designs are secure.

International security standards need to be taken into account. ISO 27001 is one such standard and gaining accreditation in this is a significant advantage for any cloud provider.

WHAT IS THE NEW CHALLENGE?

Cloud infrastructure requires a fast, dedicated, scalable, efficient and resilient network. Each of these is equally important to support Service Level Agreements (SLAs) for customers.

1. **Speed**: Cloud-based solutions can take advantage of very high speed interconnects that would be very expensive to provision direct to a company office.

2. **Dedicated**: Direct links between the cloud and the customer guarantees performance, and improves security by removing the public Internet risk. Where applications and data are separated, a direct link limits the latency.

3. **Scalable**: All applications have traffic peaks which can sometimes be managed through the Quality of Service (QoS) mechanisms. Where QoS is not enough, additional bandwidth and links have to be provisioned.

4. **Efficient**: QoS and traffic shaping help manage network traffic. This is important for mission-critical applications that need guaranteed bandwidth at busy times.

5. **Resilience**: Multiple network circuits into both the data centre and the customer provide scalability and business continuity.

For a service provider, having access to multiple network providers at the data centre means being able to negotiate lower prices based on larger bandwidth requirements. It also ensures the availability of multiple circuits for disaster recovery.

Network Security

Network security is a major challenge. Traditional solutions rely on firewalls for protection. As virtualisation has matured, firewall and security have taken advantage of it. Recognising the speed with which VMs are created and deployed, vendors have created rule-based virtual firewalls that can be kept constantly updated and deployed on demand.

The key here is 'constantly updated'. Normally when a VM is shutdown, it is not possible to maintain the firewall or security components. Now, there are vendors that allow for a master firewall to update the elements of all firewalls, even those in shutdown VMs.

BENEFITS OF DIRECTLY CONNECTING CLOUDS

Using leased lines rather than public Internet provides a number of key benefits.

- **Speed**. Direct connections use leased line technology, a very stable, long established method of point-to-point connectivity that comes with little risk. IP based options mean that speeds have moved from 2-32Mbps to as much as 1Gbps. Some European cities are already supporting connectivity of 10Gbps. With direct connections now as fast as data centre backbones it is no longer the weak link in any cloud deployment.

- **Multiple carriers**: The risk of an outage, even with direct connection is a very real risk factor. Provisioning direct connections from multiple carriers not only mitigates risk but can also aid with speed by allowing the connections to be bonded or used for load balancing.

- **Service Level Agreements**. Direct connections have a very high SLA which can range from 99.5% to 99.99%. This equates to a downtime of between 216 minutes and 4.32 minutes per month. This compares favourably with network resilience inside most private data centres where the SLA is often 99.5% rather than 99.99%.

- **High volume data transfer**. A direct connection enables customers to move high volumes of data to and from the cloud. A key advantage of this comes when either synchronising or backing up to the cloud. With a high speed connection up to 10Gbps, it is possible to take snapshots of servers and data and move them to the cloud for disaster recovery and resilience.

As cloud vendors move into areas such as High Performance Computing as a Service (HPCaaS), a direct connection means that the vast data sets for tasks such as computational fluid dynamics, life science modelling and medical imaging can be moved without the problem of latency that occurs with lower speed circuits.

- **Enhanced network performance**. High bandwidth, low latency connectivity enables customers to treat clouds as part of the data centre for more frequent migration/replication of data, allowing for more homogenous business continuity/disaster recovery policies, and retention strategies.

- **No contention**. Private connectivity does not have problems with contention at busy times. This means that all the bandwidth is available rather than the service provider throttling the connection when many customers are using the circuit.

- **Elastic / Bursting**. Directly connected clouds make it easy to scale a connection to meet customer needs. With up to 10Gbps connections, customers can easily provision multiple connections to increase capacity as needed. With connections being predominantly fibre optic, additional capacity to increase bandwidth can be added with relative ease.

- **Security**. A direct connection between clouds increases security through the use of highly encrypted data links.

- **Pay as-you-go pricing**. Some network and cloud providers are now increasing flexibility for directly connected customers, meaning that customers pay only for the network ports and the data transfer over the connection, which can greatly reduce networking costs (and with no minimum commitment). For those who are looking at using cloud as a disaster recovery solution this allows you both a persistent connection that can be turned up as required and greater cost control.

WHAT KEEPS THE CLOUDS IN THE AIR?

Hybrid clouds can increase complexity due to interoperability issues and the need to deal with different tools, APIs, and management frameworks. Customers generally prefer familiar existing technologies, tools, and user interfaces to handle hybrid cloud scenarios seamlessly and securely.

Over the last year, all the leading management tool providers have adapted their tools to address cloud as just another deployment platform. The management applications show cloud alongside on-premise providing transparency for operations teams. This allows customers to use the tools they have and know, reducing the need for staff retraining.

CONNECTIVITY AND SERVICE LEVEL AGREEMENTS (SLA)

Cloud viability depends on reliable and fast connectivity. Establishing the level of connectivity has already been covered but what about reliability? The reliability of the cloud service is part of the SLA between the customer and the cloud service provider. But there is a challenge when the SLA is breached. Is it the network? The connection between the client and the cloud provider? A lack of bandwidth? Apportioning fault takes time.

Cloud providers who own their own infrastructure can negotiate both their connectivity to the Internet and the connectivity between their cloud and customers. This underpins the cloud provider's enterprise-level SLA with the customer. With end-to-end control the cloud provider is able to track, identify and then rectify faults.

An effective SLA requires many things; the two biggest components are adequate management and monitoring tools allied to a fault-tolerant infrastructure. These depend on the right hardware, software, choice of multiple carrier partners and data centre provider.

A key challenge of any SLA is definition:

• What does uptime mean?

• What metrics are used to assess the SLA?

Once the language has been agreed, there are other questions that often get asked such as:

• How are uptime and metrics measured and by whom – customer or cloud owner?

• What auditing is carried out of the cloud environment and by whom?

• Is 24/7 support available from a person rather than an automated fault system?

All of these should be covered by the SLA and be agreed by both customer and cloud provider.

SOLVING THE MANAGEMENT GAP

Integration of multiple computing environments has always been difficult. Cloud is just another platform for which tools need to be developed. This is where the development of federated management tools which allow customers to manage the cloud in the same tool that manages on-premise computing is having an impact. Without federated tools, enterprise developers will have to write their own management integration or rely on partners, such as system integrators to do it for them.

It is not only management tools that need to be properly integrated. Support for compliance software, end-to-end encryption of data in transit, encryption of all data in the cloud, integrated enterprise directory services, support for Application Lifecycle Management tools and governance are all enterprise requirements. The public cloud must provide solutions to all these requirements.

CHOOSE THE LOGICAL HOME FOR YOUR CLOUD

Before planning to build a cloud instance, there are key questions to ask in selecting foundational infrastructure, such as the colocation facility. If physical access is required, then it should be sited close to an SI office.. Alternative premises in the same geographical region can provide backup, business continuity and disaster recovery services. If power is an issue, the ability to switch workloads to an alternative data centre is a requirement. Location, however, is not the only element that has to be considered:

1. **Why carrier-neutral colocation offers flexibility?** Carrier-neutral colocation allows the cloud provider a wide choice of carriers to obtain services from. This range of carriers enables the cloud provider not only to manage the SLA for its service, but also ensures it reduces the latency of

its service due to the choice of connectivity. This "community of interest" bringing cloud providers, carriers and end-users together is fundamental in the successful delivery of hybrid cloud solutions.

2. **Power and cooling**: The efficiency of the data centre design in reducing power wastage and efficient cooling cost is extremely important. Evaluating different data centre designs for energy-efficiency should be a key consideration.

3. **Environmental awareness**: European legislation over carbon emissions means customers will be expecting the cloud provider to prove the green credentials of the facility. As such, cloud providers should seek a data centre provider that has a reliable, consistent access to green energy suppliers.

4. **Security**: The layers of security at colocation data centres are likely to exceed those of most smaller scale in house build data centres, as they are servicing multiple, often highly security sensitive, customers and are audited on a very regular basis.

5. **Future-proof**: Colocation offers scalability. Resources will support growth of the customer base while 'pay as you grow' means no heavy CAPEX costs.

Whether hybrid clouds are held by a single enterprise or managed by a service provider to serve multiple customers, the advantages are the same. Colocation enables them to focus on their customers, instead of infrastructure. Done right, it is the key enabler of a successful hybrid cloud offering, bringing carriers, end-users and cloud providers together into a single community of interest.

MODELS TO GROW REVENUE

For any business to undertake a change or evolution of their business model requires proof that it will result in revenue growth. We see two relatively easy wins for those system integrators who build their own cloud, professional services and specialist cloud platforms.

SKILLS SHOWCASE

Building a cloud environment showcases skills that can be sold to customers as professional services, especially enterprise customers wanting to build their own private clouds. For a systems integrator, this helps cement relationships with customers and promotes professional services teams that understand the core technologies involved in the data centre.

FROM CAPACITY CLOUDS TO CAPABILITY CLOUDS

Hybrid clouds are not the only area of interest to enterprise customers. Specialist clouds dealing with specific vertical markets or interests, such as accounting, healthcare, CRM and sports are beginning to appear. These are known as capability or community clouds. The attractiveness of community clouds is their narrow focus and the ability for service providers to develop a deep level of specialist services for both B2B and B2C customers.

There is another type of cloud focused on specific workloads. For example, analytic clouds, where the focus is on storage of large datasets and the provision of tools to do detailed analysis. These clouds tend to be massively computational, using High Performance Computing (HPC) systems, rather than commodity computers. As data analytics and business intelligence are typically key CIO topics, there is a lot of interest in analytic clouds.

Both these cloud variations share the cost of developing highly focused services across the customer base. This is very different to public clouds where many of the services are general purpose with potentially a lower utilisation.

A key differentiator with both these clouds is that they enable the cloud provider to develop more focused resource plans. As a result, the cloud provider will gain a lot of experience very quickly, thus improving services and provisioning.

GETTING TO THE BOTTOM LINE

For systems integrators and distributors, there are significant benefits from the delivery of cloud computing to their customer base. Leveraging existing skills and systems, a consistent revenue stream and greater integration with customer business requirements are examples.

Not everything has an obvious benefit. For example, shifting customer revenue from big CAPEX purchases may mean lower discounts from hardware and software partners. However losses should be short-term loss only. Providing access to resources on demand and cloud-based services via subscriptions should replace any lost infrastructure revenue.

To succeed requires an underlying hardware, software and services platform on which to build a cloud solution. This is a major conundrum for many systems integrators – build, buy or rent.

BUILD

Building a cloud infrastructure carries risk and expense. It requires facilities, hardware, software, a service layer and cloud business models. For larger SIs use of existing resources that they already own, such as managed data centre services, is an advantage.

The advantages of building a cloud are as much about defining the business as they are the opportunity. Key reasons for an SI to build include:

- Control over the entire infrastructure making it energy- and management-efficient
- Cost control through facility design and making best utilisation of the resources
- Reinforcing partner relationships, especially in the facility and communications fields
- Leveraging existing professional services business to take the experience of building a cloud platform out to customers. Professional services are a key engagement opportunity and revenue stream
- Creation of task specific or community clouds allowing the SI to focus on a niche market. This could be business- or community-centric

BUY

Buying an existing infrastructure and converting it is another option. There are a lot of second and third tier hosting providers renting rooms in existing facilities with large amounts of hardware and software. Many would like to move to cloud, but lack the right partner.

Moving them to a data centre that is cloud-ready and helping them install a cloud service layer onto their existing environments would utilise their skills and enable the SI to gain valuable experience in cloud design.

There is a risk that the hardware may be end-of-life or unable to reach the utilisation rates that cloud and virtualisation demand. There could also be contractual issues around the existing premises. These are risks that must be resolved before taking this step.

RENT

Renting, in this context, is buying space on an existing cloud infrastructure and offering a virtualised service. The challenge is ensuring that there is sufficient control and stability across the platform that is being rented.

There are examples of this working: IBM, HP and Microsoft are allowing key dealers to buy space to offer solutions for the SME market. IBM has deals with telecom partners such as A1 Telekom in Austria where IBM provides them the infrastructure for their public cloud offering.

DECISION

The most likely decision for the majority of systems integrators will be to build their own cloud using the facilities provided by an experience partner. This will ensure a solid, reliable foundation on which cloud solutions can be built. It will allow the SI to focus on their skills such as IT management and integration of solutions while the facility provider focuses on power, cooling and infrastructure.

CONCLUSION

Cloud offers system integrators a huge opportunity to move from being service-based to running their own infrastructures and widening their appeal to customers. As customers look to move away from CAPEX to OPEX across their IT budget, SIs can leverage cloud environments to enhance their relationships with existing customers and open up new markets.

Transformation of business models requires a bold approach. Companies like Apple, Amazon and Netflix transformed their business models a decade ago. Since then, record stores, book shops and video rental companies that failed to spot the trend have ceased to trade. Even those still around are struggling to adapt to the changes brought about by Apple, Amazon and Netflix.

Cloud now gives SIs that same opportunity to change their business model and transform their business. While others in IT are building out infrastructure, SIs can leverage their existing experience in integration of disparate systems and deliver an adaptable cloud model that allows businesses to seamlessly grow into the cloud.

AUTHOR BIOGRAPHIES

Ian Murphy has worked in technology as a journalist and analyst since 1983. He has written for a number of titles in computing; Computer Weekly, Techworld, Datacentre Times, IT PRO, Data Business, International Developer, Know Your Mobile, Anywhere You Go, Windows NT Magazine, EXE, and Cloud Pro. As a freelance analyst, Ian has worked for Philips Global Media, Ovum, MWD and Creative Intellect Consulting writing reports and consulting with a number of large technology businesses, writing white papers and giving keynote presentations at major IT shows.

Jelle Frank (JF) van der Zwet manages the pan-European marketing and product development programme for Interxion's sizeable and fast-growing cloud community. He has over 12 years of experience working in ICT product and business development. Prior to joining Interxion, he was responsible for product management and marketing of managed services at Imtech ICT, and was Senior Product Marketing manager at UPC. Jelle Frank began his career working in marketing management positions for KPN and Amsterdam Schiphol Airport.

ABOUT INTERXION

Interxion (NYSE: INXN) is a leading provider of carrier and cloud-neutral colocation data centre services in Europe, serving a wide range of customers through over 35 data centres in 11 European countries. Interxion's uniformly designed, energy efficient data centres offer customers extensive security and uptime for their mission-critical applications. With over 500 connectivity providers, 20 European Internet exchanges, and most leading cloud and digital media platforms across its footprint, Interxion has created connectivity, cloud, content and finance hubs that foster growing customer communities of interest

For more information about Interxion Cloud Hubs please visit **www.interxion.com**

interxion™

WP-CL-HQ-NOCLOU-HQ-eng-7/15