TECH BRIEF 2013

MANAGED SERVICES, CLOUD AND DESKTOP VIRTUALISATION ARE HOT TOPICS RIGHT NOW. DARREN BRISCOE, TECHNICAL DIRECTOR AT COMMS-CARE DISCUSSES HOW MANAGED SERVICES PRICING MODELS AND THE PUBLIC VS PRIVATE CLOUD DEBATE CAN AFFECT BUSINESSES LARGE AND SMALL.

Private vs. Public – why private offers more advantage

The private cloud is more secure with its server stored on-site, while the public cloud is more susceptible to malicious attacks such as hacking and viruses - which can ultimately compromise the safety of data.

Not a day goes by without another story about cloud computing. With so many companies looking to outsource their IT maintenance to save money, cloud offers a flexible and cost effective way to run an organisation. But cloud computing is a business model that few organisations understand fully. For a start, the 'cloud world' is a divided one, in that there are two different types of cloud environments: private and public. Both offer many benefits, but there are big differences between the two – particularly when it comes to the security of data.

Without question, the advantages of working in a private or hybrid cloud environment outweigh any disadvantages. With private cloud, companies get full access to their organisation's network from any internet enabled device, anywhere in the world. This is possible because administrators store their applications in the virtual cloud instead of a physical server. Consequently they gain full control over all their virtual servers. Space is freed up and energy costs are reduced. There's also low upfront capital expenditure and low on-going management and maintenance costs. Most importantly, there's greater security and resilience in the data centre infrastructure. Administrators can store their data privately and can access the virtual environment any time to resolve issues. The fact that the private cloud isn't shared by any other organisation generally makes it much more robust than a public cloud offering.

Public cloud is growing in popularity and some of the biggest companies in the world are already using it to store data, including Amazon and BT. However, there are many significant disadvantages that should be addressed so that users understand the risks involved. Firstly, the long term costs can add up, and may not prove to be cheaper than making an initial investment in on premises/data centre owned hardware/software solution.

Public cloud is dependent on sound internet connections and servers are stored offsite, so there's no immediate physical access. In many cases, businesses don't even know where the servers are located. They might be in countries that are politically insecure, which can threaten safety of data. Also, data is shared publically, which makes it vulnerable and the data isn't encrypted, so if there's a malware, virus or hack attack, it can be lost forever.

These issues are too great to ignore, but there are also many benefits to public cloud – particularly for small and medium sized enterprises. Public cloud is a good choice for organisations that want the flexibility of accessing applications anytime, anywhere. Organisations that may have limited access to servers or don't want to have them on-site might prefer to use public cloud. Those with large numbers of remote workers or a highly mobile workforce would also benefit. It's advised, however, that if companies do decide to use public cloud they should also understand that data is at risk and any sensitive material should be encrypted to add an extra layer of protection from attacks and data disasters.

Have managed services providers got their pricing models wrong?

When it comes to managed services, it's important to define the cost up front and offer a package. A lot of the margin for error in the price of managed services disappears when customers have a clear indication of the price and what can be delivered.

Gartner recently predicted that 20% of managed service providers will go to the wall. It's hard to disagree with this forecast. There's a feeling out there that if you don't get the managed service proposition right then providers will find themselves in trouble. But why are so many companies struggling to avoid bankruptcy? It all comes down to pricing models.

Managed service providers are rationalising their service offerings. They want to appear competitive and unique so they offer clients customised packages. The problem with this approach is that it's just too bespoke. Instead of managing expectations and cost, providers will say yes to everything the customer wants at knock down prices. Eventually the provider can't deliver against their promises or make any money.

This is easier said than done because it's difficult to price services correctly to cover costs and make a margin for the business. You could take two identical customers in terms of users, systems and set-up structure - and there will always be differences and one will cost more to service.

Businesses address the costing issue by going down the route of bespoke services, but if managed services are too bespoke organisations will always tend to push the boundaries for what service they can get and often it can't be delivered - at least not within the profit margin. That's why it's important to define the cost up front and offer a package. A lot of the margin for error in the price point disappears when this happens. If customers have a clear indication of the price and what can be delivered then it's easier to make a profit. They can see exactly what they are getting and at what price.

How do you determine the right price? The best way is to take what is considered the key parts of the managed service and offer a price package that includes the maintenance of these essential services. The cost for the service can be determined by a price algorithm that is based on the number of supported devices. This approach seems to work well for providers and their customers because it's easier to manage cost and the expectations of the customer.

Before long, customers start complaining and the managed service provider struggles to support their needs. Eventually these businesses either go bust trying to keep customers happy at the expense of going over-budget without charging extra or give up when they can't deliver the service and ruin their reputations. If they don't want to lose money or compromise their brand name, often they will continue to manage spiralling service requests, which forces the channel to quadruple its prices to recoup lost revenues.

The problem managed service providers face is that customers themselves don't know what they want. Without fully understanding what a managed service provider does, clients will turn to one and say they want support. The onus is on the provider therefore to come up with a workable solution that is effective and profitable.

The success of Comms-care's packages and celebrated customer service ties in well with the feedback we get from our partners. As long as we remain responsive to our customers' needs, are listening to them and are moving with technology and innovation - then we are going to survive and thrive. Outsourcing isn't dead, it just needs to be done in the right way. And if it's done properly it will always be cheaper for organisations to look outward for support instead of relying on a bloated, internal IT department.

Desktop virtualisation is very secure, but managed service providers must know how to minimise data risk

The biggest threats to data are actually coming from internal sources. The onus is always on the organisation to have the right level of encryption to protect their data.

There's a big push for desktop and client virtualisation as BYOD continues to grow in popularity. Unfortunately many IT departments don't know how to manage or deal with all the security implications it brings. According to a recent survey conducted by Comms-care 44% of respondents cited worries about safeguarding data as a main barrier for the adoption of BYOD.

Outsourcing BYOD support is an appealing option, but many managed services providers aren't staying close enough to the technology or keeping up with new developments to understand it well enough. Like many IT departments, service providers are also terrified of managing the security risks posed by mobile and tablet devices because they don't know what types of risks virtualised clients actually bring.

If managed service providers expect to grow in the future, they need to understand how to manage virtualised desktop environments and deal with security risks.

The good news is that it's safer to have virtualised clients on a personal device - because the security is taken care of by a centralised cloud server and not managed on a per device basis. If something goes wrong then the problem can be addressed quickly by an administrator through accessing the central area where all data is stored.

Furthermore, preventative measures can be taken before any client virtualisation software is installed to shield data from external attacks. Among the most effective ways is to invest in Cisco's Identity Services Engine (ISE). This is an all-in-one enterprise policy control platform that enables organisations to enforce compliance, enhance infrastructure security, and simplify service operations. It allows users to produce security profiles for different devices - whether it's tablets or mobiles - so they can connect to a network securely.

ISEs are installed at the beginning to eliminate all security problems coming from external threats. But are these risks exaggerated? Do most businesses actually have data that is sensitive enough to be of any value?

The fear of being hacked by an elite external mafia gang is extremely small for most businesses. Professional hackers and troublemakers are only going to go after organisations that store personal data on file and they are generally massive global organisations that have encrypted this data and stored it on a private cloud.

In reality, the biggest threats to data are actually coming from internal sources. Over 90 per cent of the greatest risks to data, such as - malware, viruses and hacking - are done by people taking things away on a USB or downloading them into personal devices.

With internal hacking, you can't just avoid the problem by installing a piece of software. It's all about security processes and how to implement policies. That's the biggest risk that's always overlooked. There's very little that can be done if an inside job has taken place and there's a security breach.

The one thing that businesses and government organisations are adhering to at the moment is an unpublished standard called the business Impact Levels (ILs). This framework provides a seven-point scale to help assess what steps organisations need to take to effectively meet their risk management requirements of confidentiality and integrity. Enforcing an IL can help to create policies that protect data and possibly deter people from stealing it - but ultimately it can't stop all attacks.

Essentially, the onus is always on the organisation to have the right level of encryption to protect data.

Virtualisation is already here and soon most desktops will be part of the environment. To speed up adoption, vendors such as Microsoft are even starting to give away virtual clients for free - and this trend will only continue. If managed service providers and IT departments are to stay in tune with this innovation they need to understand the risks and encourage end users to encrypt data.