Cloud Control

When it comes to moving mission critical systems over to the cloud, there is a common misconception that an element of control is lost. This is particularly prevalent when migrating business communication systems from an onsite to a hosted solution. However, says Dave Paulding, Regional Sales Director UK, Middle East & Africa, Interactive Intelligence, this is not the case and the cloud can actually offer businesses a greater level of control.

One of the perceived benefits of using in-house systems is that customers can configure them to their own requirements and, if necessary, have the vendor or its partners develop customer specific add-ons. In reality, legacy onsite applications were rarely designed to support extensive modifications and such an approach was inevitably expensive, risky and almost certain to increase maintenance and support fees.

Cloud vendors typically have built-in features that enable flexible configuration and options such as spare data fields allow users a degree of customer specific changes. As with any new system deployment, the process should be to identify business requirements, determine how much it would cost and what risks would be involved in having the solution customised to meet those specific needs.

In terms of cost control, contact centre executives and managers are often under severe financial pressures. For this reason most cloud-based vendors stress the cost savings inherent in transitioning to their model; namely reduced (or no) upfront capital expenditure, no annual maintenance fees, a reduction in office space, and less need for dedicated technical implementation and operational resources. In response, companies sometimes raise concerns they could be held ransom by vendors and have a reduced capacity to monitor day-to-day costs as these are likely to vary by number of users, volumes of transactions, or some combination of both.

Of course any concerns can be addressed and acquiring cloud-based contact centre functionality is in reality not dissimilar from buying an onsite solution and businesses should approach it in exactly the same way. This means taking care to choose the right vendor, tie a contract down and monitor spend carefully. Most cloud-based vendors offer the opportunity for a trial run, during which time customers can monitor their usage and thus build a better financial model for their ongoing operations. To support this, most reputable vendors offer tools for customers to monitor their usage and costs.

Another issue, more emotional than practical, is that an in-house system is physically on-site and the company can do what it likes within the bounds of the licence agreement. This is of course not the case for cloud-based systems. However, this choice comes with its own advantages. For example, a cloud-based supplier will have backup systems at different data centres, making it more secure against events such as accidents or natural disasters.

Different vendors have different approaches to the number of versions they support; some argue there should only be one and all customers should use it, while others support multiple versions for different customers or for the same customer. The key for customers is to explore issues such as: how many versions the supplier supports and for what purposes; customisation capabilities; integration with other systems; security; scalability; performance reliability; and how they can move away from the vendor should that prove necessary.

Failover and disaster recovery scenarios need to be worked through when designing any solution. The bottom line is that these are not simple matters and they all depend in part on unique customer needs. What is key is to spend a lot of time up-front to better understand and document various service level requirements.

In response to varying customer needs and preferences, flexible hosted deployment models have emerged. While not eradicating all issues, they do address many by giving customers more architectural options in order to better align with their unique needs. Specifically related to failure, for example, a very popular local control model has emerged that enables carrier circuits to terminate at the customer site, which is connected via MPLS to a hardened data centre. If the MPLS link goes down or the data centre goes offline, the local site can still take and route calls in a survivability mode with the local VoIP gateway and a media server/SIP proxy.

In this model and others, customers have their own version running on a dedicated virtual machine (VM) to help minimise the chance of one company being able to impact another. Each VM runs as a separate process on the host, with dedicated processor and memory resources. While it is unlikely one virtual machine can affect the entire host, switchover pairs are consciously split to run on different hosts.

It is important to understand: the model a vendor supports; what happens should the system crash; how the supplier schedules downtime; and to what service level the supplier can commit. It is also worth remembering in-house systems crash as well and companies that are un-prepared have suffered serious consequences.

Security is often cited as a major concern when moving to any model where the system is operated by a third-party. Physical site security is often more rigorous, recruitment and vetting policies for employees are kept to an extremely high level, systems access is protected with several hierarchies of user passwords, and data security is likewise protected. The key is to understand what a chosen supplier has in place; most businesses will be pleasantly surprised when they compare it to their own processes.

A key piece of advice is simply not to be scared of the cloud. In reality, many systems and applications have been operating in the cloud for a long time. For example, basic telephony and Internet services are in the cloud, many vendors transitioned CRM to the cloud some time ago and some of our most popular services, including Google and Facebook, exist entirely in the cloud. Moving some of the more specialised services associated with business and contact centre communications to the cloud can make it easier for customers to support functionality such as interaction routing to more diverse locations.

Companies should get smarter about who handles interactions without worrying where those resources are physically located. By placing the contact centre in the cloud, businesses have an opportunity to innovate in the ways that were previously not possible and to give users greater control over the ways in which

Dave Paulding, Regional Sales Director UK, Middle East & Africa, Interactive Intelligence