AIMING FOR THE CLOUDS

ACN DELVES INTO THE COMPLEX CHALLENGES ASSOCIATED WITH CLOUD COMPUTING

BY ALEXANDER SOPHOCLIS PIERI

→ Ashok Kumar, business director, Cloud Ecosystems.

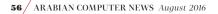→ Yasser Zeineldin, CEO of eHosting DataFort..

W hile cloud computing has flourished across the globe over the last decade, its adoption here in the Middle East has been slow by comparison. When the concept behind the technology was first introduced to the region, reactions were mixed.

On the one hand, the appeal of enhanced IT operational efficiencies and reduced infrastructure costs were favourable to many enterprises. At the same time however, many organisation avoided the jumping on the bandwagon, unsure exactly of how secure such systems really were when it came to managing back-end operations and company data.

"THE MAJOR TRAITS SEEN ARE POOR PLANNING, LACK OF COLLABORATION BETWEEN THE OPERATION TEAM AND THE IT IN CHOOSING THE CLOUD PROVIDER, WRONG EXPECTATION, LACK OF CLOUD RISK ASSESSMENT AND INSUFFICIENT DUE DILIGENCE"

ASHOK KUMAR, CLOUD ECOSYSTEMS

It was also the case that many enterprises active in the region at the time, were running operations supported by legacy platforms, which were largely incompatible with cloud. Even to date, a portion of the regional market still operates on paper-based system, making it all the more difficult to bring companies forward into the digital era.

Despite its slow start however, cloud computing has seen a substantial rise in adoption over the last five years, particularly in the UAE and Saudi Arabia. While public sector organisations still remain hesistant on the side lines, private cloud has experienced exponential growth as of late.

With its rising popularity however, new problems have also arisen. As many businesses make the push towards cloud, in many cases, the transformation is done in haste and without the proper foundation in place. This often leads into a situation, which many cloud providers describe as a 'poor' deployment.

"The major traits seen are poor planning, lack of collaboration between the operation team and the IT in choosing the cloud provider, wrong expectation, lack of cloud risk assessment and insufficient due diligence," explains Ashok Kumar, business director, Cloud Ecosystems.

Describing the right approach, he shares: "While planning to move from physical infrastructure to cloud or Hybrid, it is very important to set the goal. Understand organisation current workload and future requirements.

"THE SMB SEGMENT IS ALSO SLOWLY FOLLOWING THE TREND... CRUCIAL BUSINESS APPLICATIONS MAY OR MAY NOT MOVE ENTIRELY ONTO CLOUD DEPENDING ON THE TECHNOLOGICAL BREAKTHROUGHS IN CLOUD-BASED SECURITY SYSTEMS."

YASSER ZEINELDIN, EHOSTING DATAFORT

"Business needs to collaborate with IT in sizing the performance and end-to end service levels. Choose the right type of service that fits the business, IaaS, Paas or SaaS. After finalising on the plan of deployment, enforce security policies."

Initially entering into the market as a cloud deployment specialist, UAE-based Cloud Ecosystems later expanded its capabilities towards developing systems for cloud. Working with its clientele right from the design stage, all the way through to administration and scaling, Cloud Ecosystems' offerings include managed services, Internet-of-Things (IoT), Enterprise Asset Management (EAM), big data analytics and Customer Relation Management.

"We ensure performance of the three core technologies – compute, network and storage, similarly weighted in order to avoid bottlenecks," asserts Kumar.

"In larger enterprise or in a hybrid environment, administration of all the elements associated with service delivery, service management and monitoring tools helps our customers to keep up with the continually shifting capacity demands of a highly elastic environment."

Commenting on the security concerns of old, the business director points out that a number of flaws in data security have been addressed by major cloud providers, the best of which ensure their cloud is protected at every layer. The lingering issue he suggest however, lies with the end-user, who must remain diligent in understanding the different types of security offered, and whether it complies with the requirements of the business, as well as the region.

He argues that even if Cloud providers compile cutting-edge security controls and systems to protect their cloud, organisations remain responsible for protecting their data. Poor practices such as a lack of proper identity management, BYOD policy, and cyber threat awareness, may result in data breaches and theft. Thus organisations should remain aware of the potential hazards, as well as making an effort to devise an effective cloud security policy.

Tackling this perception of cloud security remains on ongoing challenge for fellow cloud specialist company Epicor Software. Starting from humble beginning in the Middle East back in 1996, the Dubai-based company has grown beyond the confines of the UAE, boasting over 650 customers in 40 countries, as well as over 40 value added resellers.

While its portfolio comprises of a number of ICT offerings spread across various categories, its own blend of cloud is delivered through Epicor ERP.

"The Epicor cloud solution strategy is based on two basic principles: first, providing our customers a choice in how they want to deploy their ERP software, and, second, providing easy access to point solutions that connect and extend the value of their Epicor system," explains Hesham El Komy, senior director, Channels, Epicor.
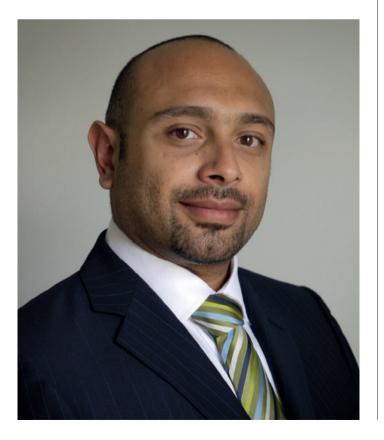
"Epicor ERP allows customers to easily migrate between cloud deployed systems and on premises licensed deployments with no impact on end-user efficiency.

"Furthermore, if customers have Epicor ERP deployed under a single- or multi-tenant SaaS model, they retain ownership of their data, and have the ability to 'repatriate' it to their network at any time."

While an enterprise resource planning system hold numerous benefits for organisations, they also unfortunately become particularly attractive targets for hackers. While financial gain is often the chief motivator behind an attack, other risks also includes hacktivism.

The term is used to describe hackers who target an entity's security flaws or sensitive customer data, as means of either discrediting the company's reputation, or as an act of cyberespionage in order to obtain access to intellectual property.

"Epicor ERP offers sophisticated application level security,

providing robust in-application as well as external security processes to protect an organisation's' critical data. These range from role based security profiles, to advanced tenancy isolation data restrictions — all operating in concert to provide both absolute control and confidence," explains Komy.

"Users are abstracted from database access, and interact with their ERP system through either the application user interface or secure web services calls, that themselves are isolated from the database by application layer business logic," he adds.

While the issue of cloud security is certainly an important topic also considered by eHosting DataFort (eHDF), the firm also highlights compliance complications around data being hosted in data centres outside of the region as a critical challenge. eHDF also highlights the lack of skilled IT talent as an inhibitor in the region's ICT development.

Despite these issues though, the general viewpoint from eHDF in regards to the GCC's cloud computing market is largely a positive one.

"The Middle East Cloud Infrastructure Market definitely

"THE EPICOR CLOUD SOLUTION STRATEGY IS BASED ON TWO BASIC PRINCIPLES: FIRST, PROVIDING OUR CUSTOMERS A CHOICE IN HOW THEY WANT TO DEPLOY THEIR ERP SOFTWARE, AND, SECOND, PROVIDING EASY ACCESS TO POINT SOLUTIONS THAT CONNECT AND EXTEND THE VALUE OF THEIR EPICOR SYSTEM."

HESHAM EL KOMY, EPICOR

is exhibiting a northward trend. Unlike the early years when cloud was nothing more than a buzzword in the region's markets, today it is for real," asserts Yasser Zeineldin, CEO of eHosting DataFort.

"The proportion of revenues being allocated to cloud computing is gradually increasing across different organizations as well. Cisco Global Cloud Index (2013-2018) whitepaper estimates the highest cloud traffic growth rate (54% CAGR) for the Middle East and Africa, followed by Central and Eastern Europe (39% CAGR) and Asia Pacific (37% CAGR)."

Incepted back in 2001, eHDF is one of the region's most recognisable providers of managed hosting and cloud infrastructure services.

To date, the company owns and maintains numerous Tier 3 data centres and is one of the few service providers to offer credit-bases service level agreements. eHDF's accomplishments also include obtaining Cloud Security Alliance (CSA) STAR Certification, reportedly the first company in the region to do so.

"The key reasons that make eHDF stand out in the marketplace is its ability to provide customised solutions that offer strategic, financial and operational benefits to customers and act as an extension to their in-house IT department," explains Zeineldin.

"eHDF's team of domain and technical experts is highly knowledgeable, committed, experienced and completely focused on keeping customers' critical applications and infrastructure working optimally without any downtime, allowing customers to focus on their core business objectives," he adds.

While pointing out that public sector organisations remain sceptical on public cloud, Zeineldin is happy to report that the popularity of private cloud is on the rise.

This is thanks in part to the fact that cloud infrastructure is proving to be more cost effective than maintaining an on premise IT infrastructure.

The model is also gaining traction amongst businesses of various sizes and focuses.

"The SMB segment is also slowly following the trend... crucial business applications may or may not move entirely onto cloud depending on the technological breakthroughs in cloud-based security systems," comments Zeineldin.

"Nevertheless, the uptake of private and hybrid clouds will definitely be higher and provide businesses umpteen reasons to invest in cloud in order to get more for less." ∎