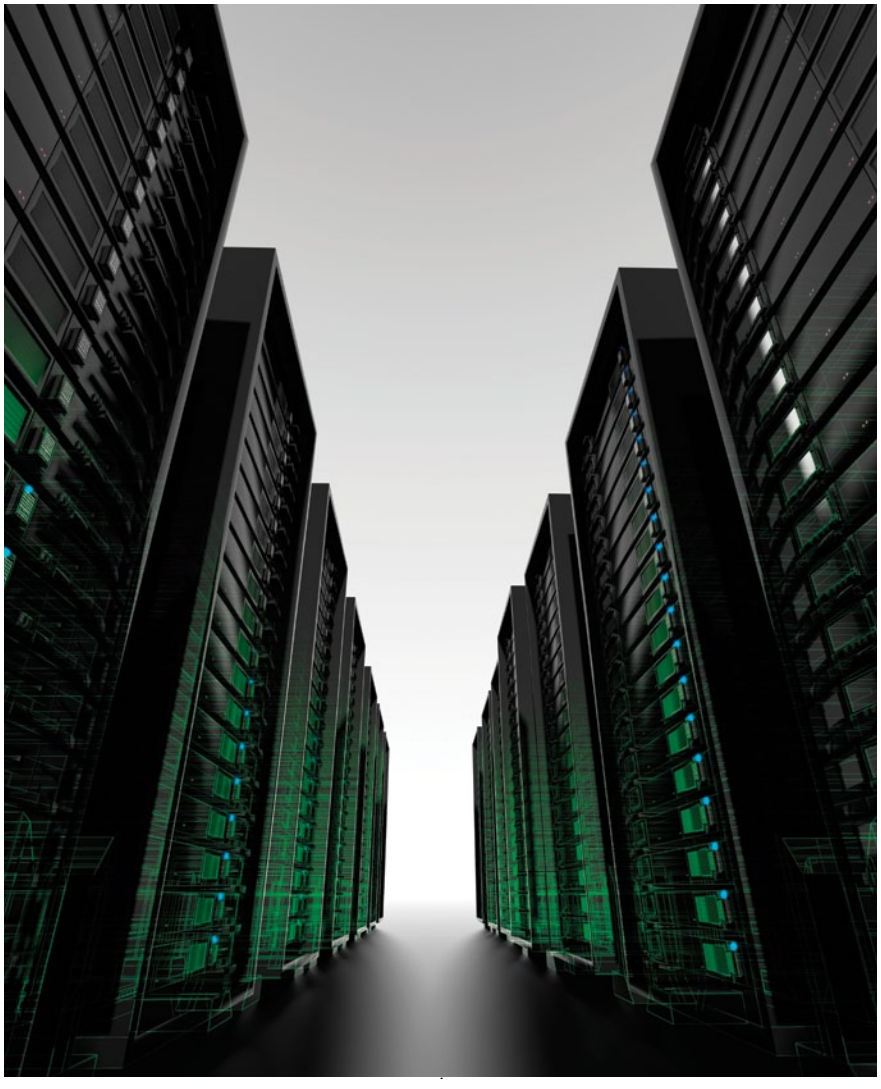
# Survival of the fittest

The past year has given enough reason for regional enterprises to begin investing in a robust business continuity (BC) and disaster recovery (DR) strategies. Vendors believe that the appearance of big data and regional regulations has had a significant impact on these strategies. CNME speaks to regional vendors to report on the state of affairs.



**Picture this. A multinational enterprise - that is worth a couple of billion dollars and provider a key service to thousand of people accross the globe - stores their financial and personal information for future reference. In a moment's notice the organisation's data centre is breached by gang of experienced cyber criminals who use the holds of customer information for identity theft or to access their bank accounts, leading to hefty personal losses. Would you be concerned? Would you be willing to work with the organisation again?**

Now picture an alternative scenario. The organisation's entire infrastructure is immobilised due to a natural disaster due to which the service it provides to you is discontinued. Now imagine this service is to do with the provision of electricity or email. How would it affect your lives? Would you be more than slightly inconvenienced?

From the popular PSN attack and earthquake in Japan to the Amazon cloud outage, over the last year a number of prominent organisations have suffered the long drawn effects of negative publicity, lawsuits and customer dissatisfaction.

Some would say, it's about time then that businesses began to realise the importance of investing in a clear business continuity and disaster recovery strategy. The need for these strategies is driven even further in a competitive environment, where margins are small and compliance standards are stringent.

Muhammed Salama, technology consultant team lead for EMC in Dubai says, "The need for a business continuity (BC) and disaster recovery (DR) strategy is no doubt steadily moving up the CIO's list of priorities due to the competitive nature of the Middle East marketplace, demanding customer expectations and the political instability across neighbouring Arab Spring countries."

"While the telecom, airline and banking sectors need to invest in a clear BC and DR strategy in order to operate in global markets, multinational organisations based in the Middle East need to create these strategies to adhere with the country's regulations," adds Steve Bailey, regional operations director at CommVault.

Sachin Bhardwaj, head of marketing and business development, eHosting DataFort (eHDF) says that for sectors like banking, finance and government, the implementation of BC and DR strategies is not about budgets but more about complying with international standards and achieving corporate governance. "Organisations today, are also looking at safeguarding their own interests as well as those of their stakeholders. So, while we do have companies spending more on comprehensive and robust DR solutions, they are also spending on back-up DR sites and provisioning workspaces should a disaster strike," Bhardwaj adds.

Regional experts agree that most enterprises in the Middle East currently invest in local DR sites with basic mirroring capabilities with some investing in sites positioned outside the primary geographic area.

**Sachin Bhardwaj,** head of marketing and business development, eHosting DataFort (eHDF)

Anthony Harrison, senior principal solution architect, EMEA, Symantec adds, "Many organisations start with a basic cold DR site and use array-based replication to keep a copy of their data offsite. However, given the complexity and interconnection of today's modern data centres, companies are realising that the data is not enough – you need a fully functional application stack to access the data and continue to run your business. That means that your DR servers need to match the logical configuration of the production ones; they may be on older or less powerful hardware but they should run the same versions of operating system, database and application."

Harrison says that there are too many things that can go wrong between a primary and DR site, so the use of analysis tools to automate the checking of DR readiness is essential in today's complex environments. "A lot of organisations have a DR site a few hundred metres away from the production one, but this only provides a limited geographical separation and could still leave both sites exposed to the same event. The majority of organisations with a production site in Abu Dhabi, for example, have the DR site in Al Ain, 130km away inland and sufficiently distant to permit operational continuity for all but the most severe of events."

Salama adds that the way regional enterprises handle their DR sites varies with regards to distance and topologies. "In a country like Egypt we find predominantly 2-site topology with distances ranging from five to below 100 kms where primary DR sites are usually located within the greater Cairo metropolitan area (few exceptions exist that exceed that range such as from Cairo to Alexandria which is just over 200km). However, in a country like the UAE it is common to exceed the 100km range as most enterprises prefer to have their DR setup between Abu Dhabi and Dubai," he says.

Salama adds that in the UAE while 2-site topology is still the norm, 3-site implementations are fast gaining ground. "In Saudi Arabia where it is common to exceed 1,000 kms and find more adoption of 3-site topologies, sites are usually located across the larger spreads of cities such as Riyadh, Jeddah and Dammam," explains Salama.

Bailey believes that the appearance of big data has also impacted the creation of robust BC and DR strategies in the way that enterprises handle data management.

## ✱ BY THE NUMBERS

**Source:** European Disaster Recovery Survey 2011, conducted by Vanson Bourne commissioned by EMC

**1750**
IT decision makers surveyed

**70%**
of UK organisations are not very confident of their ability to fully recover their systems

**43%**
of organisations in Europe suffered downtime

**89%**
stored a back-up copy of data offsite

"In the past, organisations simply created and stored information but did not work especially hard to use and mine it. Today, more organisations have begun to invest in data mining, in collating data from multiple sources, prioritising and analysing it to finally storing it appropriately. If, after all that effort, a fire erupts burning out a server with critical data, the damage will be much more significant than in years past. This makes BC and DR an essential big data strategy," he says.

eHDF's Bhardwaj adds, "While many companies are moving to disk for its reliability and faster recovery time, others have IT processes stored in tape applications. and therefore need a virtual tape library that allows them to move their processes on to disk-based backup systems either on the cloud or on their premises. We have also seen an increasing trend whereby organisations are using real time data replication solutions to replicate data from a production site to a secondary DR site."

Basil Ayass, enterprise product manager, Dell Middle East, adds that part of the reason why regional enterprises have so far lacked in their ability to create and execute robust strategies is associated with the lack of regulations regarding data movement and ownership in the cloud. "Customers are waiting for various government and regulatory entities in the region to introduce legal frameworks before they start leveraging DR and implementations," he says.

**Basil Ayass,** enterprise product manager, Dell Middle East

Harrison adds, "One of the major inhibitors for public cloud in the region has been the concern over jurisdiction in the event of any dispute or termination of a service contract with a cloud provider. Equally there are major sensitivities about copies of data leaving the country and potentially being accessible to third parties, with or without the consent of the customer or service provider."

**Laying it out**

Industry professionals believe that the first step towards creating an effective BC and DR strategy is to understand the difference between the two concepts.

"Most organisations assume that DR and BC are the same. It should, however, be understood that BC is a framework that allows the undisrupted continuity of business operations under adverse conditions, including but not limited to natural or man-made hazards, as well as hardware, human error or any other failure. DR encompasses the process, policies and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organisation after a disaster. This can be achieved by having a secondary DR site with a data replication solution. End-users must understand that DR is an essential subset of the entire BC framework," Bhardwaj says.

> "Too many vendors try to push customers into a one-size-fits-all technology choice that means vastly over-provisioned systems that do not deliver value in proportion to their business importance."

**Anthony Harrison,** senior principal solution architect, EMEA, Symantec

"For business continuity, organisations must not only look at technical solutions but also look at non-technical controls. For instance, a BC would imply minimum dependency on a particular individual to operate and maintain a critical service, so that the system remains unaffected and operates efficiently in the event of a disaster, even if one person is unable to effectively play his part," he explains.

Symantec's Harrison adds that while most organisations focus their efforts on the infrastructure and physical aspects of setting up the DR site, the application and data side is often overlooked.

"The whole purpose of the DR site is to provide access to the applications and the data that the business needs to operate, so we always advise customers to start by answering questions like is the application able to failover between servers? Is the data on shared storage (which itself will have many redundant components) so that the application can move between servers?" he explains.

According to Harrison, a mature operation will have a detailed set of recovery procedures for each application. It will specify which applications should be brought online first and for each, there will be steps to provide access to the replicated data volumes or the appropriate servers, and then bring the applications online in the correct

order. "For example, you might have a multi-tier application that needs the database to be online first, then an application server, then a web server. Such a 'virtual business service' can be brought online automatically by the latest generation of management tools, regardless of whether individual servers are physical, virtual or even on different platforms," Harrison says.

Data management experts add that business and application requirements will together define the policy associated with the data. "Businesses should start by defining their recovery time objective (RTO) and recovery point objective (RPO) and incorporating these into their implementation," says Dell's Ayass.

"Based on their RTO and RPO vendors can then translate these requirements in terms of IT complexity and cost. Organisations can then decide for instance that it wants to use synchronous replication only for the most critical systems and for those that must be recovered first. For the not-so-critical systems, organisations can use different ways to get a copy of the data offsite. For instance, they can use asynchronous replication, disk-based backup using hourly snapshots or even down to good old tape. Too many vendors try to push customers into a one-size-fits-all technology choice that means vastly over-provisioned systems that do not deliver value in proportion to their business importance," adds Harrison.

**More to come**

Regional experts have no doubt that while stringent international compliance standards will only drive the adoption of BC and DR strategies further, cloud computing technologies will perhaps most impact these BC and DR solutions in the years to come.

"With the increasing rate of adoption of data centre virtualisation technologies, as well as private and public cloud computing models aimed at improving service levels, reducing cost and increasing business agility, it will no longer be acceptable to leave expensive resources idle at a remote DR site where they may or may not be utilised once or twice a year. In addition to this, more stringent service levels and regulations will drive organisations towards the adoption of fault tolerant solutions where downtime is simply not accepted even during a disaster situation," says Salama.

"We have already seen people with dual-use DR sites; the servers are normally used for testing or development, on the understanding that in the event of a disaster, the servers will be rebuilt or re-provisioned as production servers instead. The maturing of virtualisation has made this easier to achieve as this could mean just stopping the test VMs on one server and starting up the replicated copy of the production ones instead. I also think that more and more companies will get closer to the goal of 100% virtualisation, which is a key enabler of private cloud flexibility. This eventually means we will witness the mainstream adoption of public cloud provisioning as part of an organisation's overall BC and DR strategy; while some applications will stay in house in a private cloud to deliver the ability to use resources far more flexibly," says Harrison

**Steve Bailey,** regional operations director at CommVault

Bailey concludes that as organisations come to terms with economic crunch, tougher competition and political turmoil, decision makers within these organisations will look to leverage BC and DR strategies in order to help them attain sustainable growth margins in the long run which in turn will lead vendors to new heights of innovation.

"The race to develop a self-aware BC infrastructure is not too far away. There are already many technologies that are focusing on the 24x7 continuity of the storage, data and application layers with built-in self-repair and automated decision making capabilities. We are already witnessing the development of complementary technologies that constantly monitor the 'heartbeat' and health of the infrastructure, and applications running on them to ensure a 'zero' interruption of service scenario, and this is just the very beginning," Bailey appropriately concludes. ■

> "Many organisations start with a basic cold DR site and use array-based replication to keep a copy of their data offsite. However, given the complexity and interconnection of today's modern data centres, companies are realising that the data is not enough – you need a fully functional application stack to access the data and continue to run your business. That means that your DR servers need to match the logical configuration of the production ones; they may be on older or less powerful hardware but they should run the same versions of operating system, database and application."