READY FOR DISASTER?

In October 2012, Hurricane Sandy hit New York, causing flooding in Lower Manhattan that took out several major US network hubs and data centres. Damage was caused by flooding of data centres and generator rooms, power surges, and component damage caused by inadequate cooling due to loss of power systems.

[MARIO TAMA/ GETTY IMAGES].

THERE IS GREATLY IMPROVED AWARENESS OF THE NEED FOR DISASTER RECOVERY AND BUSINESS CONTINUITY PLANNING IN THE REGION, ACCORDING TO A NEW STUDY FROM EHDF, BUT MANY ORGANISATIONS ARE STILL NOT CONVINCED OF THE ABILITY OF THEIR DR AND BC PLANS TO KEEP THEIR BUSINESS RUNNING OR BRING IT BACK FROM A MAJOR OUTAGE.

BY MARK SUTTON

High profile security incidents, and growing compliance requirements may have contributed to a rise in cyber security awareness among organisations in the Middle East in recent years, but many organisations are apparently still ill-prepared to tackle other threats to the business, specifically in the area of disaster recovery preparedness and business continuity planning.

A recent survey by hosting and services provider eHosting DataFort, in partnership with Continuity and Resilience (CORE), the Business Continuity Institute (BCI) and DNV GL Business Assurance, showed that despite increased investment in the Middle East in this field, many companies are still not confident of their ability to keep the lights on in the event of a crisis. Fifty six percent of respondents to the Middle East Business Continuity Management Survey, rated their organisation's IT DR readiness as average or below average and 64% of the respondents rated their BCM readiness as average or below average. When the same survey was conducted in 2012, over half of respondents ranked their BCM and IT DR readiness as average or below, while 41% said their crisis management readiness was average or worse.

The potential damage caused by an outage is clearly increasing, as companies become more reliant on IT for communications and operations. The top three causes for disruptions in the Middle East cited by the survey were applications and network infrastructure failure, power outage and human error, but there are any number of natural events including fire, flood, earthquake, extreme weather, and human events such as hacking and acts of war that can impact on a business. Two-thirds of respondents reported at least one significant disruption in the past 12 months, and among the survey respondents, 30% indicated that a two-day disruption to business would cost $3 million or more, according to their Business Impact Analysis (BIA) estimates.

Yasser Zeineldin, CEO of eHosting DataFort, said that the results show how the business environment is evolving: "We feel that companies have improved their approach but they still have a long way to go when it comes to a mature BCM program."

"The high cost of bandwidth in the region has put brakes on the plans of many enterprises to implement a BC or DR solution. However, there is significant awareness on the importance of such a deployment and is keen to adopt a BC/DR solution. In fact, most enterprises have put in place some sort of BC/DR plan. However, here we must keep in mind that the term is used loosely, so the sophistication level can vary significantly across different enterprises," said Gregg Petersen, regional director, Middle East & SAARC, Veeam.

Nizar Elfarra, pre-sales director, CommVault added that there are a number of factors influencing the maturity of planning: "There is far more emphasis and focus on DR/BC in the region now than there was five years ago. This is partly due to worldwide events over the last decade that have driven business to think differently about 'what do we do in the event of' scenario. For example, many of the data management conversations, meetings and presentations that CommVault has with end users have an element of BC and DR built into them — it is expected. Also, there is far

tinuity Institute, a global professional organisation for Business Continuity practitioners: "The Business Continuity Institute's annual Horizon Scan survey showed just how seriously BC professionals take cyber threats and it is encouraging to see that the importance of Business Continuity is now being recognised at the board level. Organisations are beginning to realise the value of having an effective business continuity management programme and the return on investment it can provide."

Investment in disaster recovery and business continuity has been increasing in the region. The survey showed that 27% of respondents spent between $100,000 and $250,000 on their BCM program, while 22% spent up to $1 million. The big spenders in the banking, oil and gas, telecoms, government and e-commerce sectors, which accounted for 11% of survey respondents, typically have BCM budgets in excess of $1 million.

It is necessary however, to make the distinction between business continuity and disaster recovery, as while the two are interlinked, there are different priorities and requirements for investment in the two. Zeineldin points out that DR is ahead in the region in terms of investment: "Interestingly, IT DR readiness levels are higher than BCM — indicating that organisations in the past have typically ensured IT robustness before putting in place BCM robustness (i.e. resilience of facilities, people, infrastructure, supply chain, assets etc)."

"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 natural or man-made hazards, as well as hardware, human error or any other failure. Disaster recovery (DR) is the process, policies and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organisation after a disaster.

"Therefore, a BC plan is not only a disaster recovery tool that focuses on recovering what is lost and reversing damage. For busi-

more focus on BC in the tenders that end users issue as they realise that they have to think about the 'what if' factor as well as the 'here and now' factor," he said.

"Another consideration today for the enterprises in the Middle East are the competition and compliance factors from the various worldwide markets that these organisations operate in. For example, there are standards and trading expectations within the telco, airline and banking sectors that need to be followed in order for these enterprise organisations to operate in global markets. Multinational organisations based in the Middle East are having to create business continuity programs that will allow them to adapt to the regulations of the country in which they do business in. That is why there is such activity around creating standards and procedures," he added.

Business continuity is gaining recognition at the C-level, according to Lyndon Bird, technical director at the Business Con-

ness continuity, organisations must not only look at technical solutions but also look at non technical controls e.g. depending on a single person for a critical service could be threatening during a disaster, hence training an additional person might become important.

Elfarra said that the differences between BC and DR can be reflected in the levels of investment required.

"Whilst at first glance, the two topics may be regarded as the same, they are different and separated by how much the organisation is willing to invest to keep their service on the road in the event of a disaster. A disaster recovery strategy is expected to recover your business or service within a given timescale after an interruption to service or disaster. A business continuity strategy ensures that the business and/or service seamlessly continues in the event of an outage. This strategy would typically require a considerable amount more investment in high availability infrastructure, for example, geographically dispersed data centres, high availability hardware and synchronous replication/failover software storage technology."

Organisations need to strike the right balance in spending on infrastructure and tools, and on developing skills, planning and consultancy. The survey showed that 47% of BCM budgets in the region are being spent on IT disaster recovery infrastructure, seats, software and licensing. DR and BC were originally promoted as a technology solution by vendors, Elfarra noted, and although understanding has grown that technology is just one part, there is still a long way to go before before BC best practice becomes standard for most organisations in the region.

"Undoubtedly, the ability to use technology is a very important aspect of business continuity, but it is one of many vertical components of the entire operational environment. Consider the facilities, personnel, equipment, supplies, etc., all of which also play a key role in restoring operations. The regulatory bodies have also recognised this and have clearly pointed out that business continuity planning is about maintaining, resuming, and recovering the business, not just the recovery of the technology and the associated service."

"One of the main factors that organisations overlook in BC/DR planning is people. For instance, if there was a disaster in the entire building, the data has been safeguarded. But, what happens to your people? Assuming that everyone comes out safe and they go to the DR site. Are there desktops? Are there laptops? Desks? Chairs? Internet? This is the biggest thing that I see people overlooking. It's not just about the tools and infrastructure, it's also about the relocation of people to ensure business continuity," Petersen added.

The survey does suggest that the holistic nature of BC planning is being embraced by many more companies than before, with 74% of organisations reporting that they have a dedicated BCM team, compared to just 37% two years ago. Responsibility for business continuity management is also typically not purely IT's responsibility, but is being driven by the information security units, quality management, IT and operational and overall risk teams.

Organisations are also turning to BCM tools to automate the implementation and management of their business continuity plans. The survey showed 51% of respondents either already used automated tools or were planning to evaluate them, Zeineldin said, and there are a number of advantages to deploying such solutions.

"The advantage that a BCM tool offers over and above a manual

← Petersen: Many companies overlook the people factor when it comes to disaster recovery planning.

"A BUSINESS CONTINUITY PLAN IS NOT ONLY A DISASTER RECOVERY TOOL THAT FOCUSES ON RECOVERING WHAT IS LOST AND REVERSING DAMAGE. FOR BUSINESS CONTINUITY, ORGANISATIONS MUST NOT ONLY LOOK AT TECHNICAL SOLUTIONS BUT ALSO LOOK AT NON TECHNICAL CONTROLS."

process is that it allows timely reminders to be set, automatically escalates preparedness gaps and open issues/risks/threats, avoids inconsistencies and duplication, and reduces effort by allowing for changes to be updated across multiple documents in a consistent and speedy manner, and facilitates ownership of the BCMS by individual department users, rather than allowing them to delegate to the central BCM team the ongoing maintenance and improvement of their department BCMS."

Another area of technology which has had a considerable impact on BC and DR approaches has been the rise of virtualisation. Virtualisation has made replication of servers and storage much easier, and much more affordable.

Elfarra commented: "Virtualisation has been a game changer for many companies. It has enabled companies that previously were unable to afford high availability (HA) and DR to begin implementing HA and DR solutions. Virtualisation has also enabled companies to justify the cost of providing full HA and DR for additional applications. In addition, it has provided more flexibility and more options in providing the HA and DR solution. The business challenge is having the ability to create a cost effective, highly available, and protected virtual server infrastructure. This infrastructure must ensure that applications meet business defined service level agreements (SLAs) for HA and DR preparedness."

Virtualisation has also had an impact on another area of BC and DR, the growth of third party DR services. Many companies already used third party providers for DR provisions such as offsite storage of backup tapes, but with virtualisation making it considerably easier to shift workloads, third party providers offering managed services, DR-as-a-Service, Backup-as-a-Service and other services are growing considerably. Thirty percent of Middle East organisations said they planned to outsource parts of their DR programs to specialist providers.

Petersen said: "Customers can leverage best of DR/BCM technology at fractional costs. Service providers can afford first class data centre facilities and infrastructure, and attract the crème de la crème of IT talent. The cost is spilt across multiple customers, which ensures that customers pay less for top-notch quality."

"For those organisations which do not have their own IT Disaster Recovery infrastructure, there are now multiple options on offer by Middle East-based service providers. These service providers offer secondary Disaster Recovery sites through world-class data centres, state-of-the-art infrastructure and high-quality managed operations," Zeineldin added. "These service providers typically provide assurance regarding their competence by compliance to world class standards related to BCM. So 'lease' is a good and cost effective option to consider, for those who do not want to build their own secondary IT infrastructure.

"Specialised service providers also offer options to sign up for Work Area Recovery (WAR) — backup seats to be used when the organisation faces a business disruption. These seats could be offered on either a dedicated/shared basis. For those organisations which prefer dedicated seats, the cost may be much higher than shared seats. Third party service providers can offer the advantage of economies of scale, because organisations can simply sign up for the number of seats that they need, rather than having to build a full-blown infrastructure. The Middle East also has a number of service providers who offer world-class infrastructure and high-quality managed operations, almost on a plug-and-play basis," Zeineldin concluded. ■