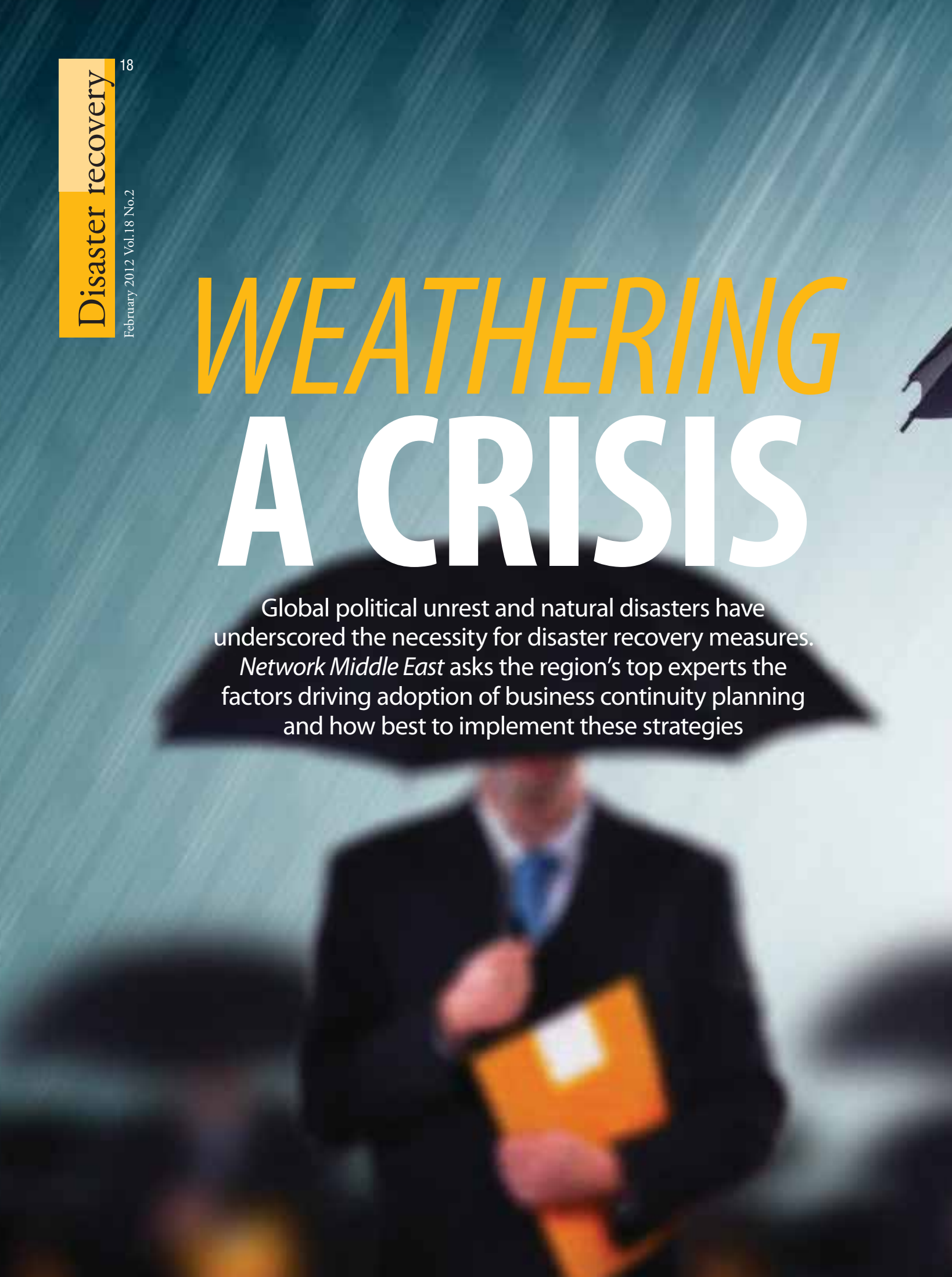
February 2012 Vol.18 No.2

WEATHERING A CRISIS

Global political unrest and natural disasters have underscored the necessity for disaster recovery measures. *Network Middle East* asks the region's top experts the factors driving adoption of business continuity planning and how best to implement these strategies



A crisis will often happen with no prior warning. At the start of 2011, for example, few could have forecast the civil unrest that swept the likes Egypt and Tunisia, countries that are often seen as bastions of stability in a perennially unstable region.

The business impact of this unrest has been huge. According to figures published by consultancy Geopolicy at the tail-end of 2011, the so-called 'Arab Spring' has cost regional economies more than $55 billion so far.

What is more, a recent survey by virtual office solutions provider Regus found 40% of businesses in the Gulf region do not have a disaster recovery strategy in place should their critical IT facilities go offline during a crisis.

Disaster recovery is already common practice in mature markets, but the concept is perhaps less well understood in the Middle East. Put simply, disaster recovery involves implementing IT systems and business processes that ensure critical technology continues to function in the event of an outage. These range from the exotic - earthquakes and floods – to electricity blackouts to human error. Disaster recovery facilities are usually provisioned from an external site away from the organisation's primary location or another country altogether.

One expert says that awareness of disaster recovery in the region is gathering pace. "There is far more emphasis and focus on disaster recovery and business continuity now than there was five years ago," believes Steve Bailey, regional operations director at CommVault. "This is partly due to worldwide events over the previous decade that have driven businesses to think differently about 'what do we do in the event of' scenarios."

Steve Bailey, regional operations director, CommVault

Bailey agrees that considerations such as regional unrest have played a role in increased adoption, but there are more mundane factors at work. "[One] consideration today for enterprises in the Middle East is 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 telecommunications, airline and banking sectors that need to be followed in order for these enterprise organisations to operate in global markets."

Bailey believes any business continuity strategy should include details on what constitutes a disaster and what needs to be done to re-instate IT systems. "The key objective of a disaster recovery plan is to detail the key activities required to reinstate the critical IT services within the agreed recovery objectives. The most effective start point for any disaster recovery plan is the 'declaration of a disaster'- once an incident has been deemed serious enough that repair at the primary location is impractical, or is likely to result in an outage longer than the maximum tolerable outage.

Critically, Bailey says, businesses should ensure the recovery plan for their IT systems co-ordinates with their overall strategy for managing business continuity in the event of a crisis. The strategy should be tested regularly to ensure it is effective and employees and key stakeholders should know their responsibilities. "A successful transition to a business continuity site ultimately depends and is linked to the disaster recovery plan.The plan should interface with the overall business continuity management plan, be clear and concise, focus on the key activities required to recover critical IT services, be tested, reviewed and updated on a regular basis, have a member of staff who takes ownership and enables the recovery objectives to be met."

> "There is far more emphasis on DR then there was five years ago"

TOO HOT TO HANDLE

Provided that a disaster recovery plan is in place, in the event of an outage IT systems will fail-over to a redundant site away from the business's primary location. The extent to which back-up systems are provided from the second site, and how quickly, is determined by whether the site is a 'hot', 'cold' or 'warm' one.

A hot site is the most comprehensive solution, but also the most expensive. "Ideally, a hot site will be up and running within a matter of hours or even

less," explains Sachin Bhardwaj, head of marketing and business development at eHosting DataFort. "However, personnel may have to be moved to the hot site. It is possible that the hot site may be operational from a data processing perspective before the staff are relocated."

The hot site will be a complete replica of business's primary IT, including hardware and up-to-date data over the wide area network (WAN).

"This type of back-up site is the most expensive to operate," Bhardwaj adds. "Hot sites are popular with organisations that operate real-time processes around-the-clock such as financial institutions, government agencies and eCommerce providers."

In contrast, a cold site is the most inexpensive method of setting up disaster recovery capabilities. Unlike a hot site though, this does not come with redundant infrastructure, but is rather the physical space to install back-up systems.

"It does not include backed up copies of data, nor does it include hardware that is already setup. The lack of hardware contributes to the minimal start-up costs of the cold site," explains Bhardwaj. "However, it requires additional time following the disaster to have the operation running at a capacity close to the original."

A compromise between a hot and cold recovery site is a warm facility, which has hardware and connectivity, but on a smaller scale than the original site. These sites may have data back-ups on hand, but they may be incomplete and days or weeks old. Back-ups may also be conducted manually, with tape volumes being couriered between the main site and the redundant one.

Bhardwaj says that businesses must assess their requirements before plumping for a hot, cold or warm site. "Choosing the type of disaster recovery site depends on an organisation's cost versus benefit strategy. Hot sites are traditionally more expensive than cold sites, since most of the equipment the company requires is purchased, which makes the operational costs higher. However, in case of an eventuality, if the same organisation loses a substantial amount of revenue for each day that they are inactive, it may then be worth the cost."

Sachin Bhardwaj, head of business development, eHosting DataFort

UNREST ASSURED

One expert says that he expects adoption of business continuity system to rise in the wake of civil unrest in the Middle East. "Geo-politics has played a big role in getting people to start looking at disaster recovery," believes Ahmed Tawfiq, executive manager, data centre, at Abu Dhabi-based managed services provider Injazat Data Systems. "Not only locally, but also cross-country disaster recovery because of the instability and the Arab Spring and everything that is happening around us."

Tawfiq says that businesses in other countries in the region could view the UAE specifically as a safe haven for backing up their critical IT systems and data. While this seems like a good idea on paper, he warns that the network links between countries in the Middle East are not always best suited for this purpose.

"The only prohibitor that is playing a big role in not being able to go cross-country in DR are the WAN links," he goes on. "The bandwidth is getting better and better but the challenge from a Middle Eastern perspective is the charges for this link, especially for a high bandwidth requirement.

However, what companies are doing that we are seeing is that, for instance, if it has a branch in Abu Dhabi or the UAE, they already have the link so they can take advantage of that."

The civil disobedience seen across the Arab world over the past 12 months is a stark, if exotic, reminder that business disruptions can and often do come from nowhere. But with the cost of downtime running into potentially thousands of dollars for each day lost, few can argue that it does not make sense to be prepared for any eventuality.

Top tips for DR/BC

- **Keep back-ups:** Mission critical data such as financial records should not only be backed up internally, but should also be replicated to an external site. Any loss can land your organisation in hot water with regulators and inflict irreparable reputational damage

- **Appoint stake holders:** In any disaster recovery strategy, it is vital to ensure there are stake holders who are designated responsibilities ensuring processes and policies are up-to-date. For example, there should be an employee for ensuring regular testing and so on

- **Act before it is too late:** It is impossible to implement a disaster recovery strategy after the disaster has already happened. Assume that a crisis could happen tomorrow and prepare accordingly. An outage could strike at any time and the costs can be massive

- **Stay up-to-date:** As your organisation changes, so should your disaster recovery strategy. Recently virtualised your infrastructure? Then your business continuity planning must reflect this