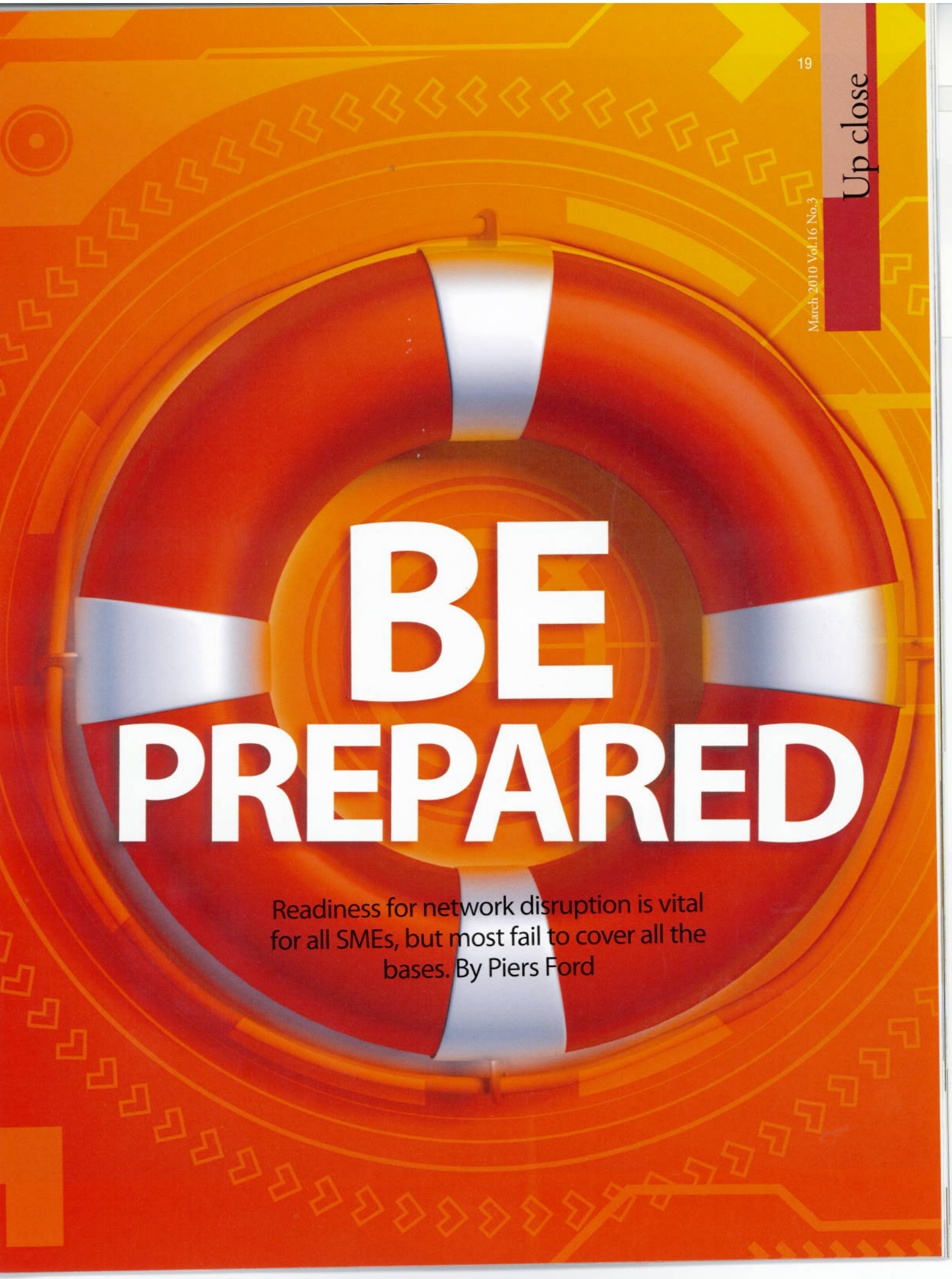

BE PREPARED

Readiness for network disruption is vital for all SMEs, but most fail to cover all the bases. By Piers Ford

Small and medium sized businesses are confident to the point of smugness that they are ready to face IT disaster. But the reality is that an alarmingly small number of them actually have all the bases covered in terms of planning for disruption. And most of them have little appreciation of the impact that any system outage is likely to have on their customer relationships.

These were the stark findings of security specialist Symantec when it published its 2009 SMB Disaster Preparedness Survey last September. The report canvassed the perceptions and practices of 1650 SMBs around the world.

More than 80% of respondents declared themselves at least somewhat satisfied with their disaster plans. A similar proportion said they were at least somewhat protected in case of disaster. Two thirds blithely reckon their customers will bear with them when their systems are unavailable. Only 34% think clients might actually go elsewhere!

However, according to Symantec, the average SMB had suffered at least three outages during the previous year, mainly because of virus and hacker attacks, power failure or natural disaster. Yet less than half the SMBs surveyed actually have a plan to deal with specific events. Data backups tend to be infrequent and incomplete. Many SMBs acknowledge that they would lose 40% of their data if a fire took out their systems.

Price to pay

The grim statistics keep on stacking up: outage costs could be as high as $15,000 per day – a huge hit for any customer-facing business; and a quarter of respondents have lost important data during an attack or disaster.

The greatest irony is that while the majority of SMBs felt their perception of their own IT suppliers was damaged by downtime – and 42% have actually switched vendors because they felt their technology was unreliable – they also felt their own customers would either "wait patiently until our systems were back in place" or "get what they could, but would wait patiently for the rest until our systems were back in place."

If there is any good news in this bleak picture, it is that nearly 90% of SMBs asked said they would create a formal disaster preparedness plan within the next six months. In reality, those good intentions have probably been superseded by numerous other day-to-day IT challenges. Not surprisingly, vendors see disaster recovery as a good platform for pitching products and services. But in the Gulf, how is this translating into action on the front line?

"It really all depends," says Sachin Bhardwaj, head of business development at hosted service provider eHosting DataFort. "Ongoing trends in the region suggest that disaster recovery has been a solution implemented across the finance and services sector.

"However, following the global economic downturn, along with a number of recent regional devastations [Cyclone Gonu in Oman, and a significant power outage in one of the Emirates, for example], organisations other than those in the banking, finance and service sectors, are more ready to take on proactive planning than ever before.

"A Business Continuity Planning survey conducted in the last quarter of 2009 is a testimony to the recent interest in business crisis planning as it revealed that companies in the region are concerned with business disruptions including failure of computer hardware, software and data loss – all perceived as the highest risk. 21% of the region's business executives also said that natural disasters such as storms, flood and earthquakes were of particular concern."

Sachin Bhardwaj says that organisations are becoming more aware of the need to prepare for network outages.

Must do more

But this isn't enough. Bhardwaj points out that 70% of the region's businesses don't have robust business continuity plans. Some have paid the price: multi-billion dollar and market share losses, and even closure, were the consequences of Cyclone Oman.

The options are clearly defined: in-house disaster recovery, which usually requires a second site, linked across an IP or Fibre Channel network, with cross-site backup and a degree of replication; leased datacentre space, which retains ownership of the infrastructure; outsourced services, which can be scaled according to the criticality of different types of data; and software as a service (SaaS), which delivers storage and software on a utility model (disaster recovery is delivered as part of the Service Level Agreement).

"For disaster recovery solution, organisations need to devise a strategy on how business objectives can be achieved, what methods and procedures need to be taken should a disaster strike, and what documents are required in the process," says Bhardwaj.

"Generally speaking, smaller companies' key constraint is cost. In spite of growing awareness of major disruptions and disasters caused to businesses in the region, companies are still not able

to fully realise the consequences of a potential disaster. While these threats are considered too remote or too unlikely to happen for it to be taken into account, business crisis planning such as the implementation of disaster recovery solutions is not on top of the SMB's agenda."

Clearly, it should be. That means stepping back and looking at the bigger picture – anticipating the impact of disaster and prioritising data recovery as part of an overall continuity plan, rather than just focusing on the kneejerk reaction to disaster when it strikes.

"Financial services companies can best understand the difference between disaster recovery and business continuity," says Carrie Higbie, a consultant with network infrastructure specialist Siemon, which has many customers across the region.

"A hypothetical company's disaster recovery plan entails nominal protections such as offsite backups, cold spares and important phone numbers for carriers and service providers. If the company's facility was destroyed by the disaster, offsite storage in a safe place would help, but if some data was waiting to be backed up when the event occurred, then all of the work since the last backup would have to be redone. Information about some new accounts would probably be lost.

Higbie suggests that when disaster struck, the business would not only have to face the challenge of reinstating day-to-day operations, but it would probably be under more pressure from customers, all of whom might be requesting information because of the same disaster that had brought the business to its knees!

"Our hypothetical company should ask itself some questions. How will the business function while recovery is taking place? How will it communicate with its customers? What is the chain of command and notification for internal staff? Where is the command centre? Is there a strategy for dealing with the increased customer demands stemming from a disaster while trying to efficiently continue its own operations?"

Outsourced solutions

Business continuity planning depends on exposure and available resources, Higbie explains. "Some companies get together and offer to provide redundant equipment for each other. The newer trend is to outsource a disaster centre or a redundant data centre. This option, while optimal, is not always fiscally possible."

Hosted services are emerging as the likeliest contender for SMBs, although it's important that network decision makers don't see this as a delegation of responsibility. They still need to take ownership of the planning and – another much-neglected aspect of disaster recovery – regular testing to ensure that the plan will be adequate if it needs to be activated.

"Comprehensive disaster recovery planning allows an organisation to identify the threats and vulnerabilities, and quantify potential critical data loss," says Sachin Bhardwaj. "In assessing a cost versus threats analysis, companies are able to visualise the potential loss and act accordingly should a disaster occur."

Managed service providers like eHosting DataFort are driving disaster recovery awareness in the gulf, offering comprehensive health checks that help the customer assess system availability and data prioritisation.

Bhardwaj says that businesses are definitely waking up to the responsibilities they have to themselves and their customers in the event of network and IT service disruption. Businesses that have already taken action are understandably reluctant to publicise their plans.

"We are running disaster recovery sites for a few customers but cannot disclose too much information considering confidentiality agreements," he says. "However, we are seeing a lot of traction from several industries where availability of data is critical for the company to operate its business successfully and downtime is not permissible, whether of the applications, the IT infrastructure or the datacentre itself."

TOP TEN TIPS FOR DISASTER RECOVERY PLANNING

Brace Rennels, technical marketing manager at workload optimisation specialist Double-Take Software – which numbers several Middle Eastern financial institutions among its customers - says there are ten important tips for any forward-looking IT manager to take when planning for disaster recovery in 2010.

1 - Getting started – this requires executive and stakeholder buy-in. "It is important to be prepared as you will need to cost justify by presenting some number that identifies the cost of downtime and how much company revenue is at risk if business systems become unavailable for an extended period.

2 - Why you need a plan – for asset protection, and the rapid recovery and restoration of business critical systems.

3 - Defining the right plan – understanding what keeps your business running and prioritising the recovery of different systems.

4 - Spot the mistakes – insufficient time spent identifying, planning or preparing for the design, implementation and exercising the system. "Every time a system update or change control process is sinitiated, the business continuity plan should be retested to see if it has been impacted and still functions as designed."

5 - Learn from real life. What happens when the UPS doesn't kick in? "Even though you have a backup plan, you don't necessarily have a backup!"

6 - Understand your business – don't skip the initial business impact analysis; not all servers have equal priority. Think communications, messaging and customer-facing systems.

7 - Know the cost of downtime – it will help you sell the need for network and infrastructure improvements to executives.

8 - Getting data out of the building – whether you outsource or invest in a secondary datacentre. "You have to plan for the worst case scenario, and if you don't, you are doing your company a disservice and putting it at risk.

9 - Think beyond tape . "Many companies are replacing tape backup solutions with disk-to-disk backup solutions because the data is readily available and it greatly reduces the recovery time typically associated with tapes.

10 - Consider enhancing business continuity with virtualisation. "The biggest excuse for not testing is the usual downtime required of the production systems in order to test the failover and recovery process." Virtual machines allow you to test virtual infrastructure as if it is part of your disaster recovery centre.