In the safety zone

With the outages costing dearly, business continuity and disaster recovery are emerging as top priorities for regional businesses. Here is what you need to know to plan right

Anthony Harrison, Senior Principal Solution Specialist – Storage and Server Management, Symantec

Businesses are generally confident about the resilience of their IT systems – until disaster strikes and disruptions ensue. Most f the businesses in the region have experiences significant network disruptions during the last 12 month, either in the form of political turmoil, power loss, hardware failures or a loss of telecom services to facilities. Most of these disruptions could have been reduced or avoided by implemented by implementing a more comprehensive business continuity and disaster recovery plan.

To compensate for the unexpected and account for the unpreventable, prudent organisations utilize business continuity products and services plans to keep their enterprises up and running in emergencies, and implement disaster recovery plans and programs against the possibility that a computer, server, office or entire building becomes unusable as a result of a catastrophe.

Business continuity and disaster recovery technologies are becoming less expensive and easier to use, in part because they are being integrated into larger IT systems, and also because they're increasingly taking advantage of aspects of cloud computing and virtualisation. There are many factors that driving this as a top technology priority for organisations in the Middle East.

"Enterprises today are facing the perfect storm. Challenging economic times are compelling businesses to achieve even greater levels of cost savings and operational efficiency. Yet business-critical applications still require vital data to be protected and available to meet increasing service-level demands. The majority of businesses that fail to protect their critical applications don't get a second chance, and those that fail to reduce their operational expenses may suffer the same fate. All these factors driving the prioritisation of business continuity and disaster recovery as top priority," says Ahmed Hassan, Area Technical Manager, NetApp Middle East.

Wouter Vancoppenol, Regional Sales Director of Double-Take (now part of Vision Solutions), adds another perspective: "Business continuity is an increasing concern for enterprises locally - they are following the same company growth and user demand curves that we have seen in other regions. This requirement for services to be available at all times is a pressing one, and means that companies

Mohamed Rizvi, Manager- Information Security and Advisory Services at eHosting DataFort

are looking at developing how their business can survive through a disaster through investing in high availability and / or disaster recovery planning and solutions.

He points out at the industries in the region that have been successful especially banking and finance has seen a huge demand for business continuity as more services are rolled out via the internet to online users. "Internet banking requires that systems are available around the clock, which has made investment in continuity part of a wider company strategy. Other industries like has seen the same business driver - customers are more demanding, and they won't accept downtime."

It is important for CIOs to make a distinction between business continuity and disaster recovery, which are often thought of as the same thing. Disaster recovery is about re-establishing IT services in the face of large-scale hardware failure or sabotage, facilities failure and/or regional natural disaster. Disaster-recovery capabilities are measured by the amount of time it takes to re-establish services and the amount of data loss. Business continuity is the ability to continue operations with little or no downtime in some of these scenarios.

"These two different perspectives on the same core problem – how do I deal with an event that is unlikely to happen but could be big enough to threaten my business? Disaster recovery has tended to be viewed as data replication, and business continuity extends that idea to include the servers, their configuration, the office space and equipment and indeed the complete business process," says Anthony Harrison, Senior Principal Solution Specialist – Storage and Server Management, Symantec.

He cites the example of a telco, for which DR could include the system that houses all of their call data records so they do not lose track of their primary revenue source, but business continuity would include the application to generate the bills at the end of that month, the printers to print the completed statements and the people to send them in the post to ensure that the company's cash flow is not impacted.

Tareque Choudhury, Head of Security Practice and Professional Services MEA, BT Global Services

Mohamed Rizvi, Manager- Information Security and Advisory Services at eHosting DataFort, defines DR as an arrangement related to the preparation for recovery or continuation of technology infrastructure, which is critical to an organisation during a disaster. "It is a sub-set of business continuity and focuses on IT systems that support business functions."

While many regional businesses believe they are prepared for an unplanned network disruption, many are not – and yet the most common causes of IT outages are addressable by having a well-defined DR plan in place. What should companies keep in mind while formulating a plan? "The main requirement should be to determine the value of data and infrastructure you are trying to protect with DR. Understanding the value is key to determining the funding an organization would put forward for their DR strategy," says Tareque Choudhury, Head of Security Practice and Professional Services MEA, BT Global Services

Harrison from Symantec says that taking the simplistic view of "just copy the data offsite and we'll worry about the rest later" represents a very high cost in terms of duplicated storage requirements (usually of the same model of high-end array), because there is no appreciation of the business value of the data. "We always advise a more granular approach to understand the business value both of the data and the applications that access it."

According to Vancoppenol, the first step is to understand what your critical applications are- that the business relies on in order to be profitable. These are the first that should be protected, either through deploying high availability or disaster recovery solutions. The second is to know what platforms you are running: even smaller organisations tend to have a mix of different server hardware in place, which makes planning how to protect the applications running on those servers potentially more difficult. Look at how to protect these multiple platforms with one tool, rather than having different products for each one. This is a more cost-effective approach, and secondly it makes it easier to spot any potential gaps in the DR plan, he adds.

With the cost of downtime going up, sometimes even battening businesses down, the pressure on IT organisations is now more than ever to ensure their DR plan is ready to go and unfailingly reliable. Think you are ready about just about anything? Think again.