

How to tackle uncertainties

It has become more important than ever for businesses to put a strong disaster recovery plan in place with built-in redundancy measures, says eHostingDataFort's **Yasser Zeineldin**

Organisations globally have become more susceptible to threats such as natural/environmental disasters, sabotage, power outages and cyber-attacks than ever before. Hence it has become even more important for businesses to put a strong disaster recovery plan in place with built-in redundancy measures, so that their data has a security blanket after unforeseen business interruptions.

Although the costs for these backups, replication, inventory and servers are high, the alternative would prove to be much more expensive and damaging. The business could hit a single point of failure, where apart from operational shut-down and financial losses; the organisation could also suffer huge damage to its reputation.

STEPS TO TAKE TO PROTECT THE BUSINESS

It is important for an organisation to proactively plan ahead to ensure that critical services and data can be accessed even during the disruption period. They need to create and maintain a business continuity management (BCM) program that will help ensure that the organisation has the resources and information needed to tackle these disruptions head-on.

Most organisations assume that disaster recovery (DR) and business continuity (BC) are the same. BC is a framework that allows the uninterrupted 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. 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 business continuity framework.



Therefore, a BC plan is not only a disaster recovery tool that focuses on recovering what is lost and reversing damage but also a proactive way to plan and be prepared should a disaster strike. For business continuity, organisations must not only look at technical

“THE OBJECTIVE OF EVERY BCM PROGRAM SHOULD BE A STATE OF PREPAREDNESS, WHERE GOALS, PARTICIPANTS, ROLES AND RESPONSIBILITIES ARE DEFINED.”

“A BC PLAN IS NOT ONLY A DISASTER RECOVERY TOOL THAT FOCUSES ON RECOVERING WHAT IS LOST AND REVERSING DAMAGE BUT ALSO A PRO-ACTIVE WAY TO PLAN AND BE PREPARED SHOULD A DISASTER STRIKE. FOR BUSINESS CONTINUITY, ORGANISATIONS MUST NOT ONLY LOOK AT TECHNICAL SOLUTIONS BUT ALSO LOOK AT NON-TECHNICAL CONTROLS.”

solutions but also look at non-technical controls. For example, depending on a single person for a critical service could be threatening during a disaster, hence training an additional person might become important.

BCM is a process to identify potential threats to an organisation and create effective back-up strategies to protect the company, its employees, and all stakeholders. The objective of every BCM program should be a state of preparedness, where goals, participants, roles and responsibilities are defined.

Since the technologies and environments change constantly, it is important to continuously update and renew the BCM process as new threats and risks appear. The organisational approach, initiated by the top management, should be holistic and methodical and include the following concrete steps to integrate BC within the organisation:

- Understanding that BC is closely linked to threats and revenue losses.
- Understanding the business lifecycle.
- Gaining an insight into revenue generating services.
- Creating different teams.
- Assigning responsibilities to each team member.
- Offering clarity on the business functions and services that are applicable to BC.
- Understanding the criticality of these services.
- Clearly determining protection levels for critical business services.
- Developing continuity strategies
- Evaluating recovery mechanisms.
- Documenting recovery procedures in the event of disruption.
- Exercising, maintaining plans, and incorporating learning into the plans.

BCM is crucial for any organisation as it looks beyond handling the disaster itself and takes into consideration the requirements to get the business up and running as soon as possible. BCM failure affects both the organization and the people working for that organization. Some of the benefits of investing in BCM are:

- BCM enhances IT readiness and business resilience, and reduces risks
- Disaster recovery management is simplified for organisations. It

can help reduce data centre operations costs and CAPEX spent on hardware

- Minimises the effect of a disruption on the business and reduces the risk of financial loss
- It better workforce relations and organisational awareness of risks, and best methods to tackle crises
- It helps meet legal, statutory and compliance obligations.
- A strong BCM program, when properly implemented, saves an organisation from business downtime and improves its reputation and trustworthiness in the long run.
- BCM programs from quality service providers often come with strong auditing tools.
- It helps maintain a strong public image in the aftermath of crisis and protects a company’s market position and helps with customer and client retention. Overall, BCM helps a company uphold its corporate responsibility and market value.

Hence we would recommend that organisations put strong BCM processes in place to help the organisation be prepared for any potential disaster, ensure that business continuity is maintained and reduce the risks to the business when disaster strikes. ■

Yasser Zeineldin is CEO of eHostingDataFort.

BCM IN THE MIDDLE EAST

eHostingDataFort’s 2014 BCM survey, conducted in partnership with Continuity and Resilience (CORE), the Business Continuity Institute (BCI) and DNV GL Business Assurance highlights the following interesting developments in the Middle East:

- 64% of Middle East-based survey respondents have established internal BCM policies or plans while 27% are considering issuance.
- 27% of the respondents invest \$100,000 to \$250,000 to implement and sustain their BCM program, while 22% invest between \$250,000 and US\$1 million.
- Large organisations in the banking, oil and gas, telecoms, government and e-commerce sectors accounted for the 11% to have set aside BCM budgets of more than \$1 million.