WEATHERING A CRISIS

By Maslina Daud and Zahri Yunos
National ICT Security and Emergency Response Centre (NISER)
(This article was published in STAR InTech on 31 Jan 2006)

Have you ever wondered how long it would take your business to get back on track if your IT system crash? What impact would it have on your company's revenue and reputation? How long can you tolerate the downtime? How can you ensure your organisation complies with the regulations, guidelines or best practices directed by the authorities?

A well thought out and properly tested IT Disaster Recovery (ITDR) plan is crucial for dealing with these questions and may potentially damaging circumstances. ITDR plans help ensure an organisation's networks and computer systems are fully functional at all times and continues providing its services without an intolerable delay. But many seem reluctant to implement ITDR plan in their organisations due to the wrong impression that it takes a large commitment in the budget and company resources.

One of the most important factors in developing an ITDR plan is getting full support from top management. Their support and commitment is significant to ensure you have enough budget and the necessary resources throughout the implementation process. But convincing top management certainly isn't easy. You need to properly justify the potential losses and additional expenditure would have to bear as well as returns and long term benefits of having ITDR plan in dealing with a crisis.

After approval from the top management comes the most comprehensive part in developing the ITDR plan - Risk Assessment. The process starts off with the identifying of important assets and is accomplished by assessing the impact of its loss to your organisation. Assets here are not only physical but

also include people, key processes and applications amongst others. Next, look into the controls that have implemented. Are they sufficient? If not, identify additional controls to those assets that would minimise those risks. Each weaknesses or vulnerability must be examined and proper countermeasures as well as controls need to be in place.

Another significant process to be conducted is Business Impact Analysis. This process involves identifying critical applications that would cause the greatest impact to your organisation should they fail to function appropriately. The analysis should include an impact study based on adverse scenario such as the total loss to premises, people, records and assets. Recovery Time Objective (RTO) which defines the maximum allowable downtime of these critical business applications will be determined during this process. Recovery strategies are then developed based on prioritised critical applications identified.

The establishment of alternate site is another critical element in ITDR plan. An alternate site is a separate location where business facilities can be accessed by the organisation as a backup whenever the primary site is inaccessible or unreachable. There are, however, several criteria that need to be considered when deciding on a suitable alternate site. While there are various options available, the selection of alternate site is normally based on each organisation’s own disaster recovery strategy. It is important to keep in mind that it is not always necessary to have an alternate site fully functioning round the clock.

Upon successfully developing the plan, it is important that the plan be exercised or tested to ensure it works as intended if ever a disaster occurs. The testing phase should also focus on the people handling the system and not just the business assets involved. Not testing an ITDR plan as good as not creating a plan in the first place. The testing phase not only measures the operability of the plan but also lets everyone within the organisation familarise themselves with their roles and responsibilities in the event of a disaster.

The IT DR plan must be consistently reviewed and updated where necessary and the personnel involved should also be notified about the changes.

Awareness and training programmes are also essential for the success of an ITDR and it should be provided to all staff. Employees need to know what the plan is all about and reasons for its existence.

Although there are no legislative on ITDR Plan in place yet, there are regulatory requirements that were set-up by Bursa Malaysia, Bank Negara Malaysia and the Securities Commission for the financial sector. Progressively, Malaysian standard on Business Continuity Management (BCM) is currently being developed by the Working Group on BCM under SIRIM Berhad. It is hoped that the standard would become a catalyst to drive top management in providing full support and commitment towards a successful implementation of BCM in Malaysia, which ITDR Plan provides an integral part.