



# BCP or DRP: Discretionary or Necessity?

For many organisations disaster recovery is not a discretionary event it is a compulsory requirement. Within the Middle East most governments have now legislated for financial organisations to have disaster recovery plans in place. Without documented and tested plans in place financial organisations run the risk of having their banking licence removed.

Besides the legislative requirements, many organisations know that disaster recovery planning is just part of the cost of running a business – just like insurance. In fact, with good disaster recovery and business continuity planning in place, organisations can expect to see a reduction in their insurance costs.

It has also been Standby's experience that those organisations with good resilient and tested plans in place find that they had to install more efficient systems. For example, archive old data off their systems, reduce and redesign databases, put in more resilient hardware and networks. All of this has an up front cost but eventually will give a lower ongoing operating costs.

Resilient systems provide better service to clients. Better services to customers means more customers and more business transactions flowing through and so there is some cost benefit in having good disaster recovery planning in place.

Standby is also aware that internationally customers and those dependant on your organisation are asking for evidence of a documented and tested disaster recovery plan. No plan and these customers will take their business elsewhere or exclude the errant organisation from responding to a tender or RFP.

There is a saying which goes "to not have a plan in place is planning to failure" and this is very much the case in business continuity and disaster recovery. So we would strongly urge organisations not to consider business continuity and disaster recovery as a discretionary item but consider as it a necessity. Part of the cost of doing business. ■



# Newsletter

Date Issued: February 2009

## The role of a CEO in a disaster

In a disaster the role of the CEO changes. He or she is the figure head of the organisation. The news media and public expect you to respond and represent your organisation.

The CEO is there to make the strategic decisions. The operational and infrastructural actions are taken by the operations management people.

The following are some guidelines taken from international research on disasters.

### CEO's expected leadership

Even the most devastating or catastrophic crisis will be forgiven if the organisation is honest, open and is seen to be caring.

Behaviours in leadership throughout the process are:

- Empathy
- Oversight
- Commitment to zero
- Restitution or penance

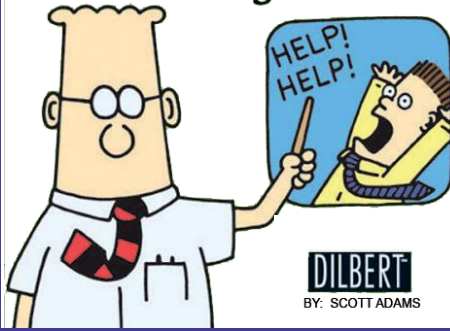
### Take responsibility for the care of victims

The single most crucial element in any crisis, aside from ending the victim-causing event, is managing it from a victim's perspective. Appropriate steps need to be taken to care for victims' needs. These are:

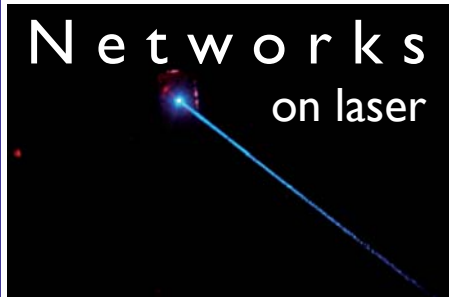
- Maintain a positive, constructive path to resolve the victim issues promptly
- Set the appropriate "tone" for the organisational response

*Continued over page*

## Our Disaster Recovery Plan Goes Something Like This...



## Networks on laser



As part of your DR and/or network capabilities you can now utilise laser technology to link LANs point to point or from building to building.

Bandwidth ranges from 100Mb to 1Gb and data can be transmitted over direct line distances from 10 metres up to 5km.

There are many benefits of using laser bandwidth including:

- No interference
- Highly secure data transmission
- No licensing requirements
- One off installation cost
- No monthly usage fees
- Cost effective and easy installation compared to traditional networks.

Laser networks offer full duplex wire speed connectivity and are IEEE 802.3u compliant. Typical applications include:

- Replacement of lower speed leased lines or radio links
- Interconnection of LANs in campus or industrial environments
- High bandwidth connectivity to the Internet and VoIP applications.

These networks can also be used for temporary installations and as an emergency back up.

Standby has a client who has recently “seen the light” and installed laser network connectivity between their site and Standby’s building. This client has found the system to be very reliable and continues to increase the amount of data that is being replicated and backed up to our site. ■

## Risk Analysis

*Incidents rarely ‘just happen.’ Rather, there is a build up of contributory factors or pre-conditions.*

When carrying out a Risk Analysis you can identify those factors and pre-conditions and take actions to reduce the exposure.

Traditionally, an IT infrastructure and facilities risk review has been considered the logical starting point when embarking on business continuity or IT disaster recovery planning project.

Today, an increasing number of organisations are also undertaking risk reviews on a more frequent basis. The primary purpose of these additional reviews is to eliminate the risk or reduce the exposure to business losses caused by a failure of critical functions.

It is essential that risk is kept to a minimum as business models change. Organisations become more reliant on IT for the delivery of customer focused Internet services, new products, applications and systems.

Another time to consider an independent review is prior to major changes of your IT location, platforms, applications or infrastructure. This review may identify risks that could be created by the changes or modifications or may suggest modifications planned.

The requirement for risk reduction is not only being driven by the need for good governance, but also by Boards of Directors, Government legislation, and customer and shareholder demands.

Standby has completed many risk review projects for clients. We have built on our experiences and take an independent, holistic approach, which often means that we detect risks and exposures that clients themselves have not identified. ■

*Continued from previous page*

This approach protects the organisation’s relationships with various constituents during the response and recovery period, shows respect for victims, and reduces the threat of trust or reputation damage.

### Commit acts of leadership at every level.

Acting like a leader is significance during urgent situations. Literally walk around and talk to people. Encourage, suggest, knock down barriers, and help everyone. Stay focused on the ultimate response process goals. Ninety percent of senior executive activity should involve first hand communication, leading, motivating, and sharing empathy. ■



© Standby Consulting (ME) Ltd 2009



P O Box 75824  
Juffair  
Kingdom of Bahrain

t. +973 17588080  
f. +973 17588080  
m. +973 36040666

[www.standbyconsulting.com](http://www.standbyconsulting.com)