



7 tips for an effective DR plan

Yasser Zeineldin, eHosting DataFort, analyses the most important aspects of an effective disaster recovery plan, in order for enterprises to best prepare for a damaging scenario.

The sinking of the RMS Titanic on her maiden voyage is one of the most famous disasters of recent centuries. Recent investigations have isolated the low grade of iron used to make the more than 3 million rivets that held the Titanic together as a significant contributing factor to the disaster. Ultimately, despite being an engineering marvel of its time, the Titanic was undone by one of the smallest and seemingly most inconsequential of its components.

The tragedy of the Titanic serves to remind us that a good disaster recovery plan ought to go beyond anticipation of the likely sources of disruption. Some of the ways in which an enterprise can prepare for failure include:

1 Planning for the least possible disruption of communication:

A methodology that allows the enterprise to maintain basic communication between departments is a must. In order to best prepare for an extreme event, an enterprise must have pre-identified alternatives to standard methods of communication and coordination, which can operate outside the realm of business as usual scenarios.

2 Clearly identified performance parameters:

Specific variations in work culture and hierarchy must be considered for the enterprise to operate well enough to recover - who is to perform what function, in the event of disruption; which individuals and departments are most critical to the containment of an event, and which functions are the priority areas to address.

3 Clearly identified roles for individuals and departments:

There needs to be well-rehearsed and clearly defined alternative roles – for individuals and departments – in the event of disruption. It is always possible to have alternative functions in place to best utilise the resources of the enterprise during an emergency.

4 Established practices and service agreements:

While the affected organisation itself is likely to act in its best interests, several outside entities – from clients to collaborators – are affected by a disaster. A well devised plan needs to be put in place to limit the damage to such entities.

5 Protecting sensitive information central to the business:

Every enterprise has operational information that can harm the organisation should it fall into the wrong hands. An effective disaster recovery plan should identify worst case scenarios that could cause such repercussions and the most optimal ways to minimise such damage.

6 Regular testing of emergency procedures for effectiveness:

If the elements that need to come together to minimise damage are not sufficiently prepared for, even the best devised disaster recovery plan can prove to be ineffective the contingency plan. Regular testing and familiarisation with the disaster recovery plan is a must so that the disaster can be negotiated with minimal damage.

7 Robust redundancy of procedures, process, entities and infrastructure:

Redundancy not only limits the range and scale of the disruption, it also reduces the chance for a disruptive disaster. While isolating functions and departments is counter intuitive and not desirable, redundancy allows for separation of these elements so that the disaster can be minimised and contained. ■