

Planning for rainy days

eHosting DataFort's Sachin Bhardwaj highlights the importance of protecting data through an effective data recovery plan

Today, the reliance of technology in a business environment spreads across every department and grows on a daily basis. While the benefits of technology can reap greater profits, at the same time, the increased dependence on technology is an indicator of the immense amounts of data that is processed within this ecosystem. IT infrastructure is built to collect, store and process critical data and encompasses the entire range of networks, servers, devices, databases, etc.

This brings along added complexity to the processes and other business elements, where, having technology/data up and running at all times is important for organisations. It is therefore imperative that companies must be in a state of preparedness for any IT disasters and address the issue by implementing a disaster recovery plan that is well cushioned with strong capabilities of data protection on a continuous basis.

Assessing the essential elements that need backup and recovery must be an important part of any disaster recovery plan wherein the recovery point objective (RPO) and the recovery time objective (RTO) are clearly defined. RPO is the minimum frequency at which data is backed up that differs for organisations and can be set for intervals of anywhere between 10 minutes to an hour. While the RTO is the maximum length of time the system can sustain the disaster before it can feel the repercussions of the disaster.

In an ideal situation, organisations must have their data protected on a continuous basis which is needed to offset their losses in the event of any disaster. This helps businesses to access and recover their data and infrastructure as quickly as possible and can ensure that the business is running as smoothly as possible.

However, while there are options which provide data recovery, they are not to be misjudged as a replacement to traditional backup. Data still needs to be backed up to an offsite location to ensure its integrity is not lost.

While it is important to have a strategic game plan for data security and recovery, it is also critical to prepare for untoward instances and have the right IT environment which is robust



←
Sachin Bhardwaj
director of
Marketing
& Business
Development,
eHDF.

enough to tackle any issues needed for data recovery with the right backup and storage facilities in an effective manner. To attain this, companies must follow systematic steps that will come to the fore in an event of a disaster.

At the start, they must assess all the data available and ascertain which is the most critical data and ensure that it is properly encrypted. It is also important to define the recovery time as this is critical in business operations and can lead to severe damage if the data is not recovered on time.

However, it is not just important to create a disaster recovery plan, it is more important to ensure that the plan is tested to guarantee the success of the plan.

Data must be regularly and automatically backed and must ensure that critical applications are available continuously which will ensure that the employees remain productive.

Companies must also ensure that their data is stored in a secure environment and therefore, it is important that the services provider must be a trusted partner so Companies can leverage the benefits of their services and boost business productivity. ■

Sachin Bhardwaj, director of Marketing & Business Development, eHosting DataFort.

“ASSESSING THE ESSENTIAL ELEMENTS THAT NEED BACKUP AND RECOVERY MUST BE AN IMPORTANT PART OF ANY DISASTER RECOVERY PLAN.”