How COVID-19 has changed business continuity planning for now and the future

Presented by
Jay | ManageEngine
Business resilience expert

ManageEngine
RecoveryManager Plus

Demystifying business continuity planning

- Business continuity is your business' ability to continue functioning as 'normally' as possible during and after a crisis.
- Essentially, it's your ability to plan for and effectively manage disruption to business as usual.
- A business continuity plan is a formalized processes to manage disruptive situations like disasters like cyberattacks, natural calamities, and even global pandemics

You can't predict the next crisis, but you can be prepared for it

- Traditional BCP focuses only on planning failover and high availabilty. That's hardly the case nowadays.
- BCP 2020: A more comprehensive approach covering organizational measures and technological aid to get back up on your feet ASAP
- Important yet overlooked aspects of BCP:

1. Disaster recovery planning
2. Business continuity testing and,
3. Crisis communication

Importance of business continuity planning

Recovering from a crisis can be very time consuming. Here's a few tasks IT leaders have to do

- Bringing the systems back online and restoring any lost data
- Replacing lost or inaccessible devices and ensuring that each can run the user's required software
- Provisioning and configuring applications.
- Designing new ways of working and communicating them to users, from alternate network access methods

Most importantly, all of these tasks are to be accomplised in the middle of an emergency

Importance of business continuity planning

With a clear business continuity plan, organizations have a clear road map towards swift business recovery and meet necessary regulatory compliance.

A few compliance that you can fulfill:

- ISO 23301
- NFPA 1600
- GDPR, HIPAA (If you take in backup and recovery planning)

Adaptation is key to resilience

When a pandemic strikes, a strong BCP can help your organization:

- Minimize the impact on staff, the organizational supply chain, service delivery and IT infrastructure
- Protect the organization's reputation
- Reduce financial impact
- Return to new normality sooner

Important aspects of business continuity planning

Mission critical data has no time for downtime! Your DR plan should ensure that your enterprise is up and running in no time after a disaster.
Failing to do so may result in the business' bottom line to take a hit.

The following three key elements ensure business continuity

1. Resiliency
2. Recovery
3. Contingency

Preventing valuable data loss

- Data loss risk can be mitigated with a backup plan in place. Thumb rule of a good backup plan is the 3-2-1 rule
- 3-2-1 rule, Backup 3 copies of your data, with copies stored in 2 different types of media and keep 1 of these copy offsite.

Most overlooked factors when backing up data

- Defining tolerance for data loss and eventually, downtime
- Defining procedures to handle sensitive information
- Cost of treating all data as mission-critical

Establishing recovery objectives

- The first step of any disaster recovery planning is to establish recovery objectives.
- To do this, you'll need two key metrics that form the corner stone of any DRP

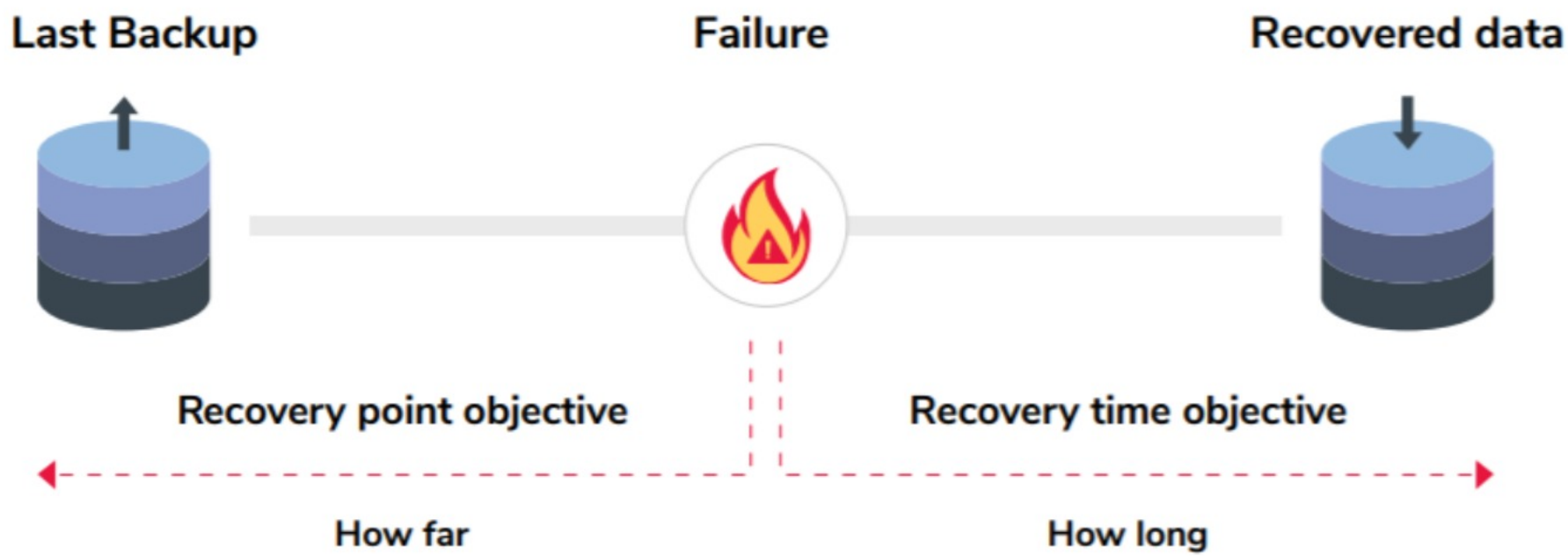
  - Recovery time objective (RTO)
  - Recovery point objective (RPO)

RTO and RPO

- Recovery time objective is the maximum amount of time business operations can be down after an outage. For critical systems and data, it is advisable to have a low RTO.

- Recovery point objective is the amount of data that an organization can afford to lose in the event of a disaster. The RPO is essential to determine the minimum backup frequency required by the organization.

How RPO and RTO's are related



Classifying and prioritizing data

Not all data in an enterprise is mission critical. It is important to classify data and define the associated metrics for retention, retrieval and archival.

Based on recovery priority, you can broadly classify data and applications as follows:

1) Non-critical
2) Business-critical
3) Mission critical

Classifying data and applications

Non-critical:

Data and applications that don't change very often. The loss of non-critical data rarely affects business continuity.

Business-critical:

Data and applications that are not required to run the business, but are more important than non-critical data. The business can continue to operate without business-critical data, albeit in a diminished state.

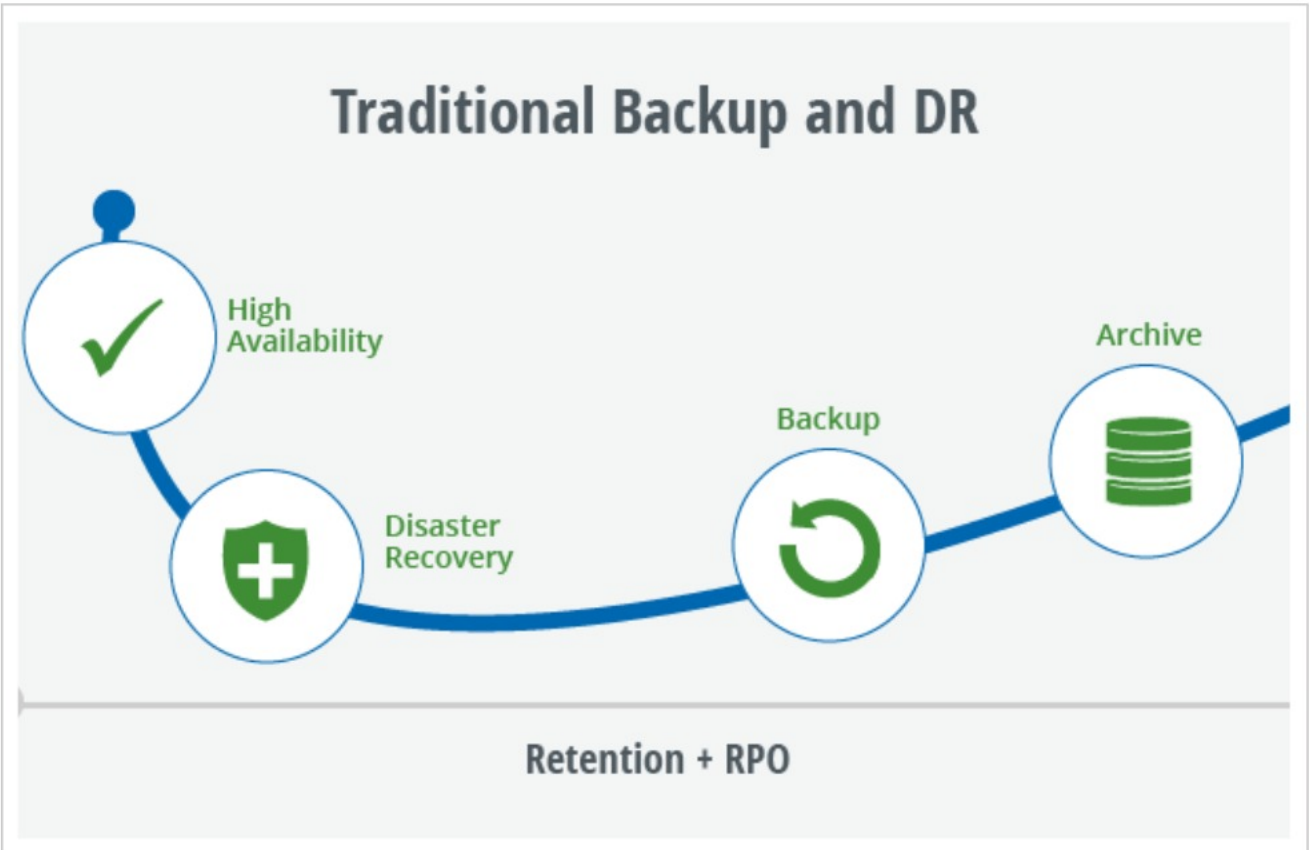
Mission-critical:

Data and applications that are critical to ensure business continuity. The business will come to a halt without mission-critical data.

Cost of treating all enterprise data as one

Not all enterprise data is mission-critical. Prioritize data based on it's importance and back them up accordingly.

Failing to do so can result in backup costs going over the roof.



Automate and orchestrate your DR plan

In the face of a disaster, manual processes simply cannot deliver the speed and efficiency that you will need.

Here is why you shouldn't overlook automation:

- Time is all important: Process automation enables faster resolution
- Communication: A streamlined workflow removes delays and improves visibility
- Possibility of human error: Scheduling backups can take a huge weight off a IT admin's shoulder thereby reducing errors

Equip yourself with the right tools

Once you have identified all key components of your backup and disaster recovery plan, classified your data, and prioritized it, it's time to choose what tools to use to implement your plan.

The following are the must-have features when you consider a third-party backup & recovery solution

1) Unified backup solution
2) Streamline backup processes with automation
3) Ability to delegate backup jobs

All-important features of a B&R solution

Unified backup solution:

Legacy backup tools are siloed, which makes it impossible to get a unified view of the backup infrastructure. A holistic solution lets you get a get a unified view of your IT infrastructure.

Automation:

Automation greatly reduces the chance of human error. The solution should let administrators schedule backups of the most recent version of your environments.

Delegation:

Modern backup solutions should allow non-admin users to initiate backup operations.

The RecoveryManager Plus advantage

Overcome any disaster caused by unwanted change in your IT environment

Unified backup solution

Quick and easy deployment

Ransomware threat mitigation

Automate AD, O365 & Exchange backups

Backup job delegation & auditing

Resources that'd be helpful

Thank you.

Write to me. Cheers.

jay@manageengine.com

ManageEngine

www.manageengine.com