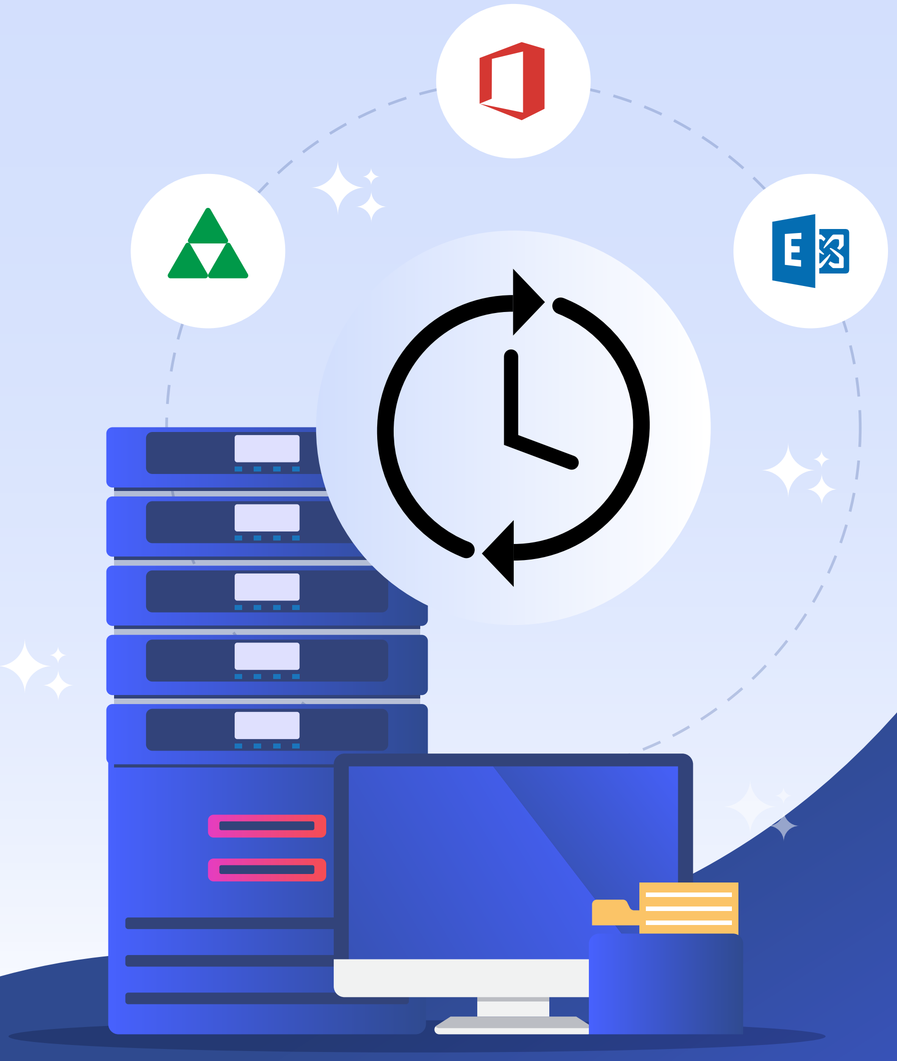
ManageEngine
RecoveryManager Plus

How to streamline your disaster recovery plan



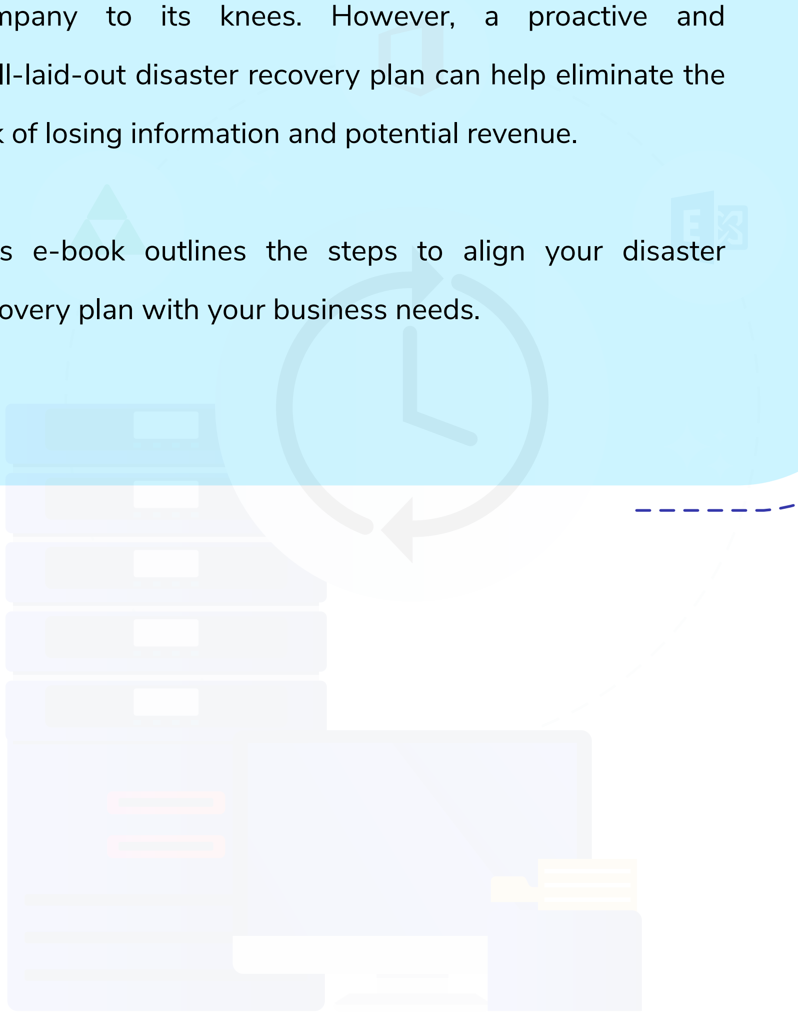
www.recoverymanagerplus.com

Index

Introduction

Disasters are bound to happen from time to time. When organizations are struck by cyberattacks like ransomware, many business-critical platforms like Active Directory, Exchange, and Office 365 are affected, bringing the company to its knees. However, a proactive and well-laid-out disaster recovery plan can help eliminate the risk of losing information and potential revenue.

This e-book outlines the steps to align your disaster recovery plan with your business needs.



Key components of a disaster recovery plan

The first step is to establish certain recovery objectives by taking into account two key metrics that form the cornerstone of any disaster recovery plan. They are:

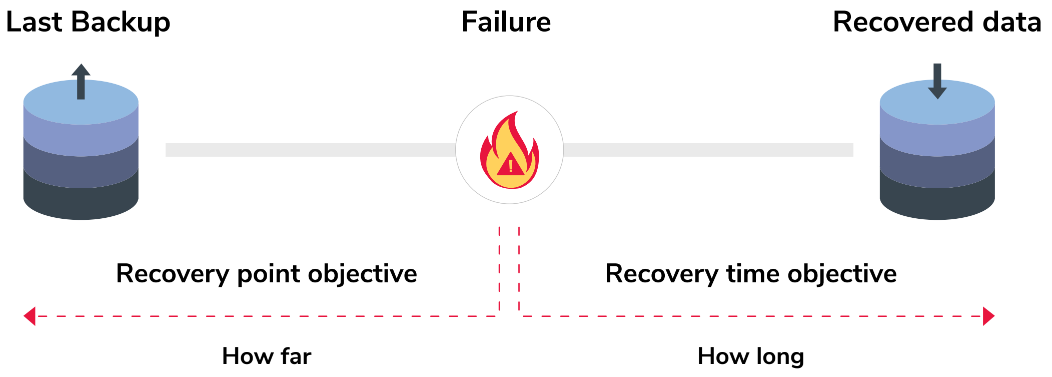
Recovery time objective (RTO)

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 (RPO)

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.

Determining both the RTO and RPO together helps with setting goals for reestablishing services before a disaster impacts the business.



Classifying and prioritizing data

In the event of a disaster, not all data in an enterprise is critical and needs to be restored immediately. One of the biggest mistakes you can make in disaster recovery planning is treating each system and process as equal. If an organization chooses to back up all its data irrespective of its criticality, costs associated with storage space can quickly go through the roof. For this reason, it's important to classify and prioritize data based on the impact it has on business continuity. This is where RPO and RTO metrics play a pivotal role.

Data and applications can be broadly classified into three categories based on their recovery priority. They are as follows:

- **Non-critical:** Data and applications that don't change very often. The loss of non-critical data rarely affects business continuity. Non-critical assets don't need to be immediately restored to ensure 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.

If an organization has a low tolerance for downtime, the RTO will be low, perhaps even seconds. Similarly, if the business can’t afford to lose any data, the RPO will be high, anywhere from hours to days.

Identify potential risks

To come up with an effective disaster recovery plan, it is crucial to identify your IT vulnerabilities and risks. One of the most common disasters is data loss, which can be the result of different data management practices—the way data is saved, stored, and handled. The following are the most common threats and risks.

1. Human error

To err is to be human. All of us are prone to making mistakes, and sometimes these mistakes prove detrimental, resulting in unintentional data loss and disrupted business operations. An employee accidentally modifying or deleting a group policy is a classic example of human error wreaking havoc. Such errors can expose your network to cyberattacks and may lead to data breaches.

2. Cyberattacks

Downtime caused by cyberattacks can often be devastating, with the company's bottom line taking a direct hit. Attacks such as ransomware can stop businesses dead in their tracks. Ransomware is malicious software designed to deny access to computer systems or data until a ransom is paid.

3. Hardware failure

Hardware equipment is highly sensitive—a server crash, drive failure, power supply failure, and natural disasters can all cause hardware to malfunction. Hardware failure can lead to file corruption or data loss. In an increasingly data-powered world, hardware is becoming the single point of failure.

Determining the right tools and techniques

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 and techniques to use to implement your plan.

There are a plethora of third-party solutions to choose from, but the following three features are must-haves when considering any backup and recovery solution.

1. Unified backup solution

Backup and recovery processes can be cumbersome. This is because legacy backup tools are difficult to manage and are siloed, which makes it impossible to get a unified view of the backup infrastructure. A holistic backup solution that lets you configure multiple Active Directory domains, Exchange organizations, and Office 365 tenants all from a single dashboard can greatly simplify backup operations.

2. Streamline backup processes with automation

A modern backup solution should function with little to no human intervention. Automation greatly reduces the chance of human error by eliminating labor-intensive tasks. The solution should let administrators schedule backups at fixed intervals to ensure you have backed up the most recent version of your Active Directory, Office 365, and Exchange environments.

3. Ability to delegate backup jobs and audit them

IT administrators already have their hands full with critical management tasks. To burden them with another responsibility is unfair. Modern backup solutions should allow non-admin users to initiate backup operations. Additionally, the admin should be able to audit non-admin user actions to ensure they're not misusing their power.

Summary

Disaster recovery comes in many forms. Ensuring the recovery of Active Directory means ensuring the recovery of your entire business. With the data and applications that drive your business all residing on top of Active Directory's services, maintaining a healthy foundation means maintaining a healthy business. If you think that creating a reliable backup and recovery system is beyond the scope of your company's resources, third-party solutions like RecoveryManager Plus can help get the job done.

RecoveryManager Plus is a web-based Active Directory backup and restoration tool that can help you overcome any disaster caused by undesired changes in your IT environment. It is a holistic enterprise backup and restoration solution that allows you to back up your AD, Office 365, and Exchange environments all from a single console.

About ManageEngine RecoveryManager Plus

ManageEngine RecoveryManager Plus is a comprehensive backup and recovery solution that empowers administrators to back up and restore their Active Directory, Office 365, and on-premises Exchange environments. With its ability to perform incremental backups, define flexible retention policies for its backups, and multiple modes of restoration, RecoveryManager Plus performs as a holistic solution to back up data that is critical for enterprises to function.

For more information, visit www.manageengine.com/ad-recovery-manager.

$ Get Quote   ⭳ Download