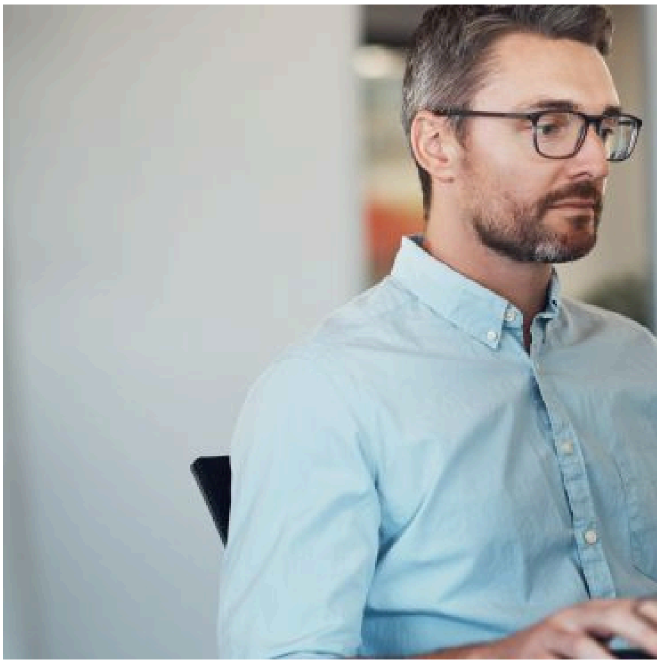
What is disaster reco



Security

What is DR?

Disaster recovery (DR) consists of I designed to prevent or minimize da resulting from catastrophic eventsfailures and localized power outage emergencies, criminal or military a

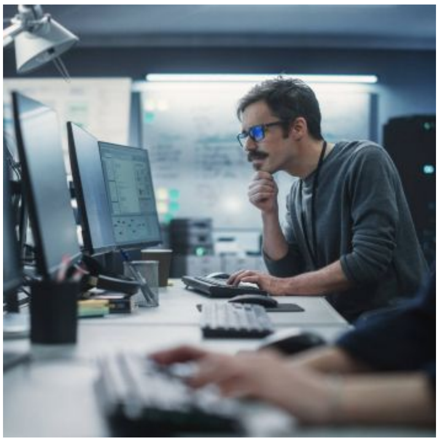
Many businesses—especially small- and mi reliable, practicable disaster recovery plan. protection from the impact of significantly d

Infrastructure failure can cost as much as U application failure costs can range from USI businesses cannot recover from such losses not re-open after experiencing a disaster, ar will fail within the first year after the crisis. I reduce these risks.

Disaster recovery planning involves strategi technology, and continuous testing. Maintai component of disaster recovery planning, b does not constitute a full disaster recovery

Disaster recovery also involves ensuring tha available to maintain robust failover and fail offloading workloads to backup systems so experiences are disrupted as little as possib original primary systems.

Read our article to learn more information a backup and disaster recovery planning.



Strengt

Stay ahea security, A

Subscr

Business continuity

Business continuity planning creates systen your enterprise will be able to maintain esse as quickly as possible in the event of a crisis is the subset of business continuity plannin infrastructure and systems.

Disaster recovery p

Business impact analys

The creation of a comprehensive disaster re analysis. When performing this analysis, you scenarios that can then be used to predict t if certain business processes were disrupte was destroyed by fire, for instance? Or an ea

This will allow you to identify the areas and critical and enable you to determine how m functions could tolerate. With this informati for how the most critical operations could b

IT disaster recovery planning should follow planning. If, for instance, your business con representatives to work from home in the af hardware, software, and IT resources would

Risk analysis

Assessing the likelihood and potential conse also an essential component of disaster rec ransomware become more prevalent, it's cr cybersecurity risks that all enterprises confr specific to your industry and geographical lo

For a variety of scenarios, including natural threats, sabotage, and employee errors, you the overall impact on your business. Ask you

- What financial losses due to missed sale generating activities would you incur?

- What kinds of damage would your brand customer satisfaction be impacted?

- How would employee productivity be im lost?

- What risks might the incident pose to hu

- Would progress towards any business in

Prioritizing applications

Not all workloads are equally critical to your and downtime is far more tolerable for some your systems and applications into three tie to have them be down and how serious the

1. **Mission-critical:** Applications whose fur survival.

2. **Important:** Applications for which you c downtime.

3. **Non-essential:** Applications you could t or do without.

Documenting depender

The next step in disaster recovery planning hardware and software assets. It's essentia interdependencies at this stage. If one softv will be affected?

Designing resiliency—and disaster recovery built is the best way to manage application i today's microservices-based architectures t when other systems or processes are down situation to recover from, and it's vital to un to develop alternate plans for your systems strikes.

Establishing recovery ti point objectives, and re objectives

By considering your risk and business impa objectives for how long you'd need it to take you could stand to use, and how much data

Your recovery time objective (RTO) is the ma restore application or system functioning fo

Your recovery point objective (RPO) is the m recovered in order for your business to resu businesses, losing even a few minutes' wort in other industries may be able to tolerate l

A recovery consistency objective (RCO) is es (SLA) for continuous data protection service inconsistent entries in business data from r tolerable in disaster recovery situations, de complex application environments.

Regulatory compliance

All disaster recovery software and solutions must satisfy any data protection and securit adhere to. This means that all data backup a meet the same standards for ensuring data primary systems.

At the same time, several regulatory standa maintain disaster recovery and/or business (SOX), for instance, requires all publicly held business records for a minimum of five year (including neglecting to establish and test a in significant financial penalties for compan

Choosing technologies

Backups serve as the foundation upon whic
In the past, most enterprises relied on tape
maintaining multiple copies of their data an

In today’s always-on digitally transforming
often cannot achieve the RTOs necessary to
Architecting your own disaster recovery sol
capabilities of your production environment
support staff, administration, facilities, and
organizations are turning to cloud-based ba
Recovery-as-a-Service (DRaaS) providers.

Choosing recovery site l

Building your own disaster recovery data ce
objectives. On the one hand, a copy of your
geographically distant enough from your he
be affected by the same seismic events, env
your main site. On the other hand, backups
from than those located on-premises at the
even greater across longer distances.

Continuous testing and

Simply put, if your disaster recovery plan ha
All employees with relevant responsibilities
test exercise, which may include maintainin
period of time.

If performing comprehensive disaster recov
capabilities, you can also schedule a “table
procedures, though you should be aware th
anomalies or weaknesses in your DR proced
previously undiscovered application interde

As your hardware and software assets chan
your disaster recovery plan gets updated as
revise the plan on an ongoing basis.

The IBM Knowledge Center provides an exa

Disaster Recovery-a (DRaaS)

Disaster-Recovery-as-a-Service (DRaaS) is managed IT service offerings available toda RPOs in a service-level agreement (SLA) tha application recovery expectations.

DRaaS vendors typically provide cloud-base significant cost savings compared with mair resources in your own data center. Contract maintaining failover capabilities plus the pe disaster recovery situation. Your vendor will configuring and maintaining the failover env

Disaster recovery service offerings differ fro their offering as a comprehensive, all-in-one

services ranging from single application res
cloud. Some offerings may include disaster
others will charge an additional consulting f

Be sure that any enterprise software applica
public cloud providers that you're working v
application performance is satisfactory in th
failover and failback procedures have been

Cloud DR

If you have already built an on-premises dis
challenging to evaluate the costs and benef
monthly DRaaS subscription instead.

Most on-premises DR solutions will incur cc
maintenance and administration, software,
upfront capital expenditures involved in the
need to budget for regular software upgrades. Because your DR solution must remain compatible with your primary production environment, you'll want to ensure that your DR solution has the same software versions. Depending upon the specifics of your licensing agreement, this might effectively double your software costs.

Not only can moving to a DRaaS subscription reduce your hardware and software expenditures, it can lower your labor costs by moving the burden of maintaining the failover site to the vendor.

If you're considering third-party DRaaS solutions, you'll want to make sure that the vendor has the capacity for cross-regional multi-site backups. If a significant weather event like a hurricane impacted your primary office location, would the failover site be far enough away to remain unaffected by the storm? Also, would the vendor have adequate capacity to meet the combined needs of all its customers in your area if many were impacted at the same time? You're trusting your DRaaS vendor to meet RTOs and RPOs in times of crisis, so look for a service provider with a strong reputation for reliability.

Read "Disaster Recovery as a Service (DRaaS) vs. Disaster Recovery (DR): Which Do You Need?" for a comparative overview of both solutions.

What is DR? Business continuity planning Disaster recovery planning Disaster Re

Report

Cost of a Data Breach Report 2024

Data breach costs have hit a new high. Get essential insights to help your security and IT teams better manage risk and limit potential losses.

Read the report →

Resources

Assessment

Cyber Resiliency Assessment

Summary

Explore IBM Storage Defender capabilities

The Cyber Resiliency Assessment is conducted through a no-cost, 2-hour virtual workshop with IBM security experts and storage architects

Learn about the capabilities provided by IBM Storage Defender to help your organization build and deliver data resilience.

Book a no-cost assessment

Read the summary

Guide

Experience Desktop as a service on IBM Cloud

Empower your remote and hybrid workforce with Desktop as a service on IBM Cloud, achieving performance and security without compromise.

Get the DaaS guide →

Webinar

The quickest way to protect sensitive data and ensure business continuity

Discover how IBM Storage Defender SaaS Essentials Edition can accelerate your approach to data resilience.

Watch the webinar

Webinar

Navigating the regulatory landscape and the impact on data protection and storage

Hear experts from IBM and Continuity Software discuss strategies for simplifying and accelerating your data resilience roadmap and the actions you should take to address the latest regulatory compliance requirements.

Watch the webinar

◀ 1 / 2 ▶

Related solutions

IBM Storage Defender

Protect your data from evolving threats no matter where it is stored with backup, AI-enabled threat detection and rapid recovery.

Explore Storage Defender →

Storage data backup and recovery

Accelerate enterprise backup and recovery processes to help retrieve data and recover IT services rapidly for on-premises and cloud workloads.

Explore backup and recovery solutions →

Cloud disaster recovery solutions

Protect your data with a cloud disaster recovery plan and mitigate the risk of downtime.

Explore cloud disaster recovery →

Take the next step

Keep your data safe and your workloads available with early threat detection, layers of protection and rapid recovery. Discover how IBM Storage Defender can help you protect your information supply chain.

Explore Storage Defender →

Book a live demo →