

What's the best way to prepare for the unexpected?

All you need to know about data protection and backup

Take control of your data protection **Protection**



is about ensuring the confidentiality, integrity and availability of data.

Carrying out backups ensures that data

is available and recoverable

when needed.



Maturity levels While this process requires thought, time and investment, you can go at your own pace with suitable, targeted actions.





Reactive, unstable and manual

REPEATABLE

Documented, standardised and reviewable **MANAGED** Proactive,

Automated, integrated and predictable

OPTIMISED

done

monitored and partly automated

Downtime & Loss

With data volumes growing exponentially, and a growing number of companies declaring themselves to be "data driven", the risks are higher than ever.

THE AMOUNT OF DATA **DOUBLES APPROXIMATELY EVERY TWO YEARS.**¹



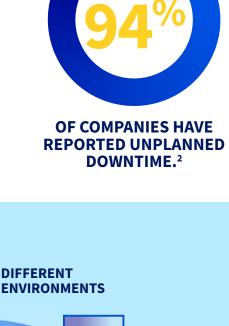
complex issue

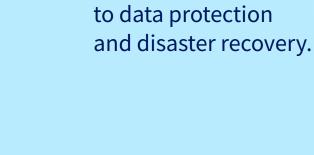
Data-driven organizations

are faced with increasing

complexity when it comes







Not just a hypothetical scenario...





During 2021

Threats to data tend to multiply and intensify.

of businesses experienced of respondents had reported that at least one experienced at least 4 such a data-related service attack had resulted in their interruptions.² data being corrupted.² interruption.²

on average per month4

And when they do occur, the consequences tend to get worse.



There are multiple sources, both internal and external. **DDoS ATTACKS**

HARDWARE phishing



Where do these threats come from?

hardware loss and theft

average time from the start of the interruption to service recovery⁴

deletions internal information leaks

ERROR misconfigurations inadequate security policies

HUMAN UNAUTHORIZED ACCESS

found that

their data was

irrecoverable.2

FAILURES OUTAGES FLOODS earthquakes **OVERHEATING** supply issues





A comprehensive data protection strategy:

applications,

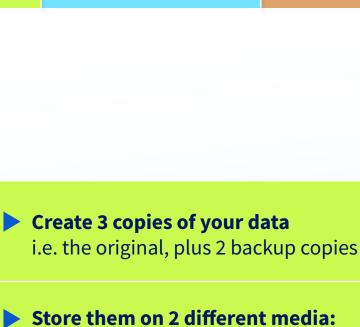
Choose an appropriate disaster recovery strategy (cold, warm, or hot scenario), or opt for a cloud disaster recovery plan (DRP) to take advantage of its benefits.

Check regularly that your strategy is always tailored to your needs, and make sure

in ransomware attacks

worldwide in 2020

compared to 2019.5



on 1 storage solution disconnected from

the rest of the network, or on 1 removable

storage, etc.

Keep 1 copy offline

storage media

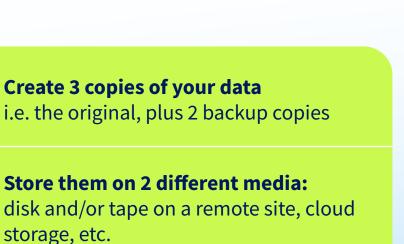
The number

of the main reasons

for requiring disaster

recovery: 56% software

failures and 47% hardware failures.2



The biggest challenge

is the reliability of

backup and recovery

operations.²



Human error

is the number



systems and distinguishing between those that are non-critical, essential, and critical?

4. Test and repeat

it works.

In the event of downtime, what will be

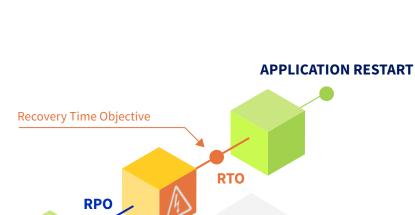
the recovery time objectives (RTOs)

and recovery point objectives for your

3. Developing a tailored strategy

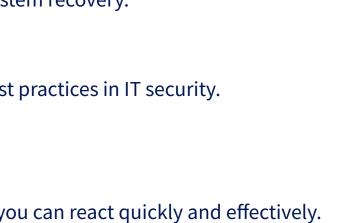
5. Document the procedures Provide clear and accurate information on every aspect of your DRP, including 6. Train and inform employees

response procedures, communication, and system recovery. Don't forget to educate your colleagues on best practices in IT security. 7. Monitor, maintain and update Be ready to detect suspicious activity so that you can react quickly and effectively. Regularly review and update your DRP to ensure it is relevant and can handle attacks and emerging issues.



Recovery Point Objective

LATEST USABLE DATA





Check the backup services included in the solutions you are using. • Move towards standard, secure storage solutions, adapted to your current and future needs (compliance, performance, price, etc.).

Before migrating

Choosing a provider

#MoveToCloud

guarantees offered in terms of compliance, sovereignty, SLA, reversibility, and so on.

OF COMPANIES WILL

BY 2025.2

HAVE ADOPTED A CLOUD

DATA PROTECTION STRATEGY

You should also consider replicating your data (copying and storing it

Before you make your choice, we advise you to note down all the

in multiple locations) to improve availability and accessibility.

- Over 20 years of expertise ► Highly resilient, certified and secure
 - An ecosystem of specialists
 - comprising the market leaders in data protection (NetApp, Nutanix, Veeam, VMware, Zerto) as well as a network of more than 1,000 partners.

interoperable services.

with no hidden fees, so you can

accurately manage your investments.

Predictable invoices,



OVHcloud

infrastructures that host integrated and

² Based on an estimate from IDC's <u>The State of Ransomware and Disaster Preparedness</u> white paper published in May 2022 ³ Based on an estimate from IBM's 2020 Cost of a Data Breach Report. ⁴ According to the annual report <u>The Cost of a Data Breach</u> published by Ponemon Institute in 2021

¹ According to Moore's Law, an empirical observation made by Intel's co-founder, corroborated by numerous research reports and studies published by the analyst firm IDC and EMC Corporation

Infographic created in June 2023

Sources:

⁵ According to the <u>SonicWall Cyber Threat's 2021 Annual Report</u>