IronTree

Understanding the basic elements of disaster recovery

Disaster recovery planning + strategy

What is a disaster and what is DR?

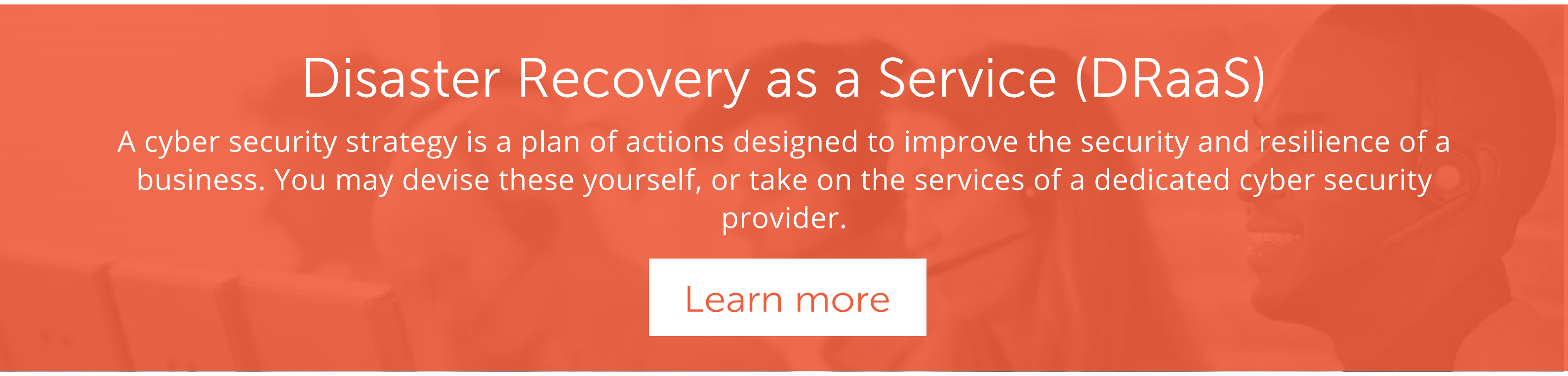
In business terms, a disaster is any event that destroys or seriously disrupts a company's resources such as its IT equipment, its data or its physical environment. The disaster may be due to theft, a natural event, human error or a cyber attack. Disaster recovery (DR) is a reactive plan of action to minimise the effects of the disaster and keeps the business running while it's being sorted out.

How to plan for a disaster in a business

1. Write down a list of your critical assets
2. List all possible disaster scenarios
3. Decide how you would protect your assets in each scenario
4. Decide who will do what
5. Create a communication plan to alert those involved in the recovery and those who'll be affected
6. Make a plan for data and systems backup

The basics of a good DR plan

A good DR plan contains a strategy for how to continue from every type of disaster. It will include a complete plan of action so that employees know their roles before chaos hits, systems can slot into place to safeguard your business operations, and your data is already backed up.



Disaster Recovery as a Service (DRaaS)

A cyber security strategy is a plan of actions designed to improve the security and resilience of a business. You may devise these yourself, or take on the services of a dedicated cyber security provider.

Learn more

Managing risk with DR

IT risk is any threat to your business data, systems and processes. A threat usually falls into one of four categories: security, availability, performance and compliance.

What are business critical (BC) functions?

Business critical functions are the apps and activities that are vital to the functioning of your business and therefore its survival. These will vary between businesses, but for most they're the functions that

- Are most affected by downtime
- Protect your irreplaceable assets
- Maintain your brand's reputation
- Maintain your cash flow

Threat examples

- **A security threat** may be the unauthorised use or access to your business data, resulting in a data breach and damaged reputation.
- **An availability threat** would mean that you couldn't access your business data or systems, resulting in reduced productivity and possible loss of customers.
- **A performance threat** would mean you couldn't carry out business operations and your productivity would suffer, leading in turn to a damaged brand reputation.
- **A compliance threat** would mean that you weren't abiding by data protection regulations, resulting in possible penalties and fines.

What is business impact (BI) analysis?

It's a system to predict the consequences that a disruption to business operations would cause. Evaluating the impact of disasters, accidents and emergencies is an important basis for investment in disaster recovery.

"RTO and RPO are important elements for working out your disaster recovery plan."

What is RTO?

RTO stands for recovery time objective and refers to the optimal time-frame necessary for restoring a business from a disruption or disaster in order to maintain business continuity (i.e. keep your business going).

What is RPO?

RPO stands for recovery point objective and refers to the amount of data loss your business can tolerate following a disaster. It examines the time between data backups and the amount of data that could be lost.

Business continuity

What is BC?

Business continuity is a proactive plan to maintain the functionality of a business as a whole. It has a wider scope than disaster recovery and includes policies, tools and procedures to manage staff and customers and prevent disruptions and disasters. In other words, business continuity is the plan that'll keep a business going over time. Disaster recovery is one aspect of business continuity planning.

What does a BC plan look like?

The template for a business continuity plan will include the steps to take for all kinds of disruptions, whether they're large like a cyber attack, fire or a terrorist attack or whether they're small like a power outage or network failure.

Critical business functions involved in BC

Your business continuity strategy will involve all aspects of your business, from its systems and assets to human resources and IT. It will consider the risks to each of these elements and set out the necessary steps to enable them to function normally when a disruption has taken place.

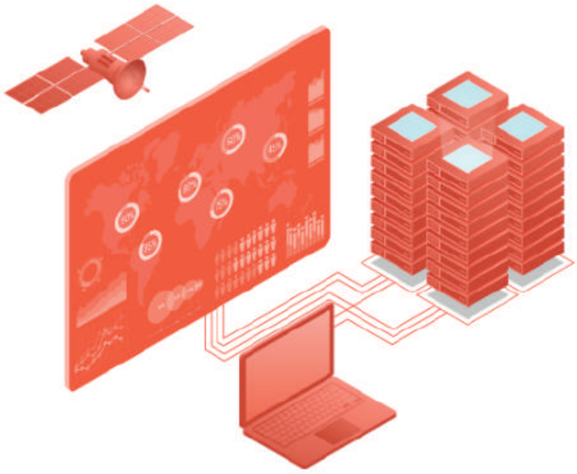
IT service continuity

IT service continuity is a part of business continuity planning that involves IT disaster recovery and overall IT resilience. It extends to the communication systems of a business and the discipline of keeping up with evolving technology.

Importance of disaster recovery in business continuity

Disaster recovery planning is a vital part of business continuity because it prepares a business for the quickest possible recovery from a disruptive or disastrous event. As cyber threats increase and a business's tolerance for downtime decreases, it becomes more and more important to have a good DR plan in place and a clear route to keeping your business going.

Data management



What does data management mean in today's age?

These days we're creating and consuming data faster than ever before. Businesses use data directly to run their businesses and indirectly to learn about trends and opportunities so they can make good business decisions.

Data management refers to the processes and policies a business uses to control its data in terms of location of data, quality, security and recoverability. It's rooted in the fact that you need to know your data BEFORE you can manage it.

Good data management enables businesses to collect, store, process, share, validate and protect data, especially personal data, in a safe, compliant and justified way.

Recovery vs prevention

Regular data backups are vital to ensure recoverability from a minor or major disruption but they don't serve to prevent a disruption of any kind. Ideally a business will have a data backup plan in conjunction with a disaster recovery plan so that it can, in the first instance, avoid a disruption and in the second, recover from one quickly if a disruption was unavoidable.

Data archiving vs data backup

Data archiving is the process of moving data that a business no longer uses to a safe storage for possible future reference or to comply with data regulations while data backup is the process of duplicating vital business documents on a regular basis so that they're retrievable in the event of a minor or major disruption.

Data management principles

The EU's Generation Data Privacy Regulation (GDPR) sets out six data management principles for businesses to abide by:

Lawfulness, fairness and transparency
Inform data subjects (i.e. the people you're collecting data about) about the type of data you're collecting and the reason you're collecting it in an easy-to-understand privacy policy.

Purpose limitation
Use data only for the purpose it was first intended and keep it no longer than is necessary to fulfil that purpose.

Data minimisation
Collect only the data that's needed for the processing purpose and no more.

Accuracy
Ensure data is kept up to date and have a way to erase or correct data that's inaccurate or incomplete.

Storage limitation
Delete data that's no longer needed for the processing it was collected for.

Integrity and confidentiality
Ensure data is protected from unauthorised or unlawful processing and against loss, destruction and damage.

Data management best practices

If you follow the GDPR's data management principles you'll be handling your data not only with integrity and accountability, but lawfully too.

A third party data management service can provide you with 'software as a service' that takes care of your backup, disaster recovery, detection and archiving needs, in a single comprehensive solution

- **Data governance** involves the people, systems and technologies needed to protect a business's data so that this data remains accessible, usable, up to date and secure.
- **Data recovery** is the process of retrieving inaccessible, lost, stolen or damaged data from a backup facility. Data recovery software used by backup providers enable a business to get its data back with maximum efficiency.
- **Data protection i**s the process of protecting important information from harm such as compromise, corruption and loss that may be due to theft, a natural event, human error or a cyber attack.