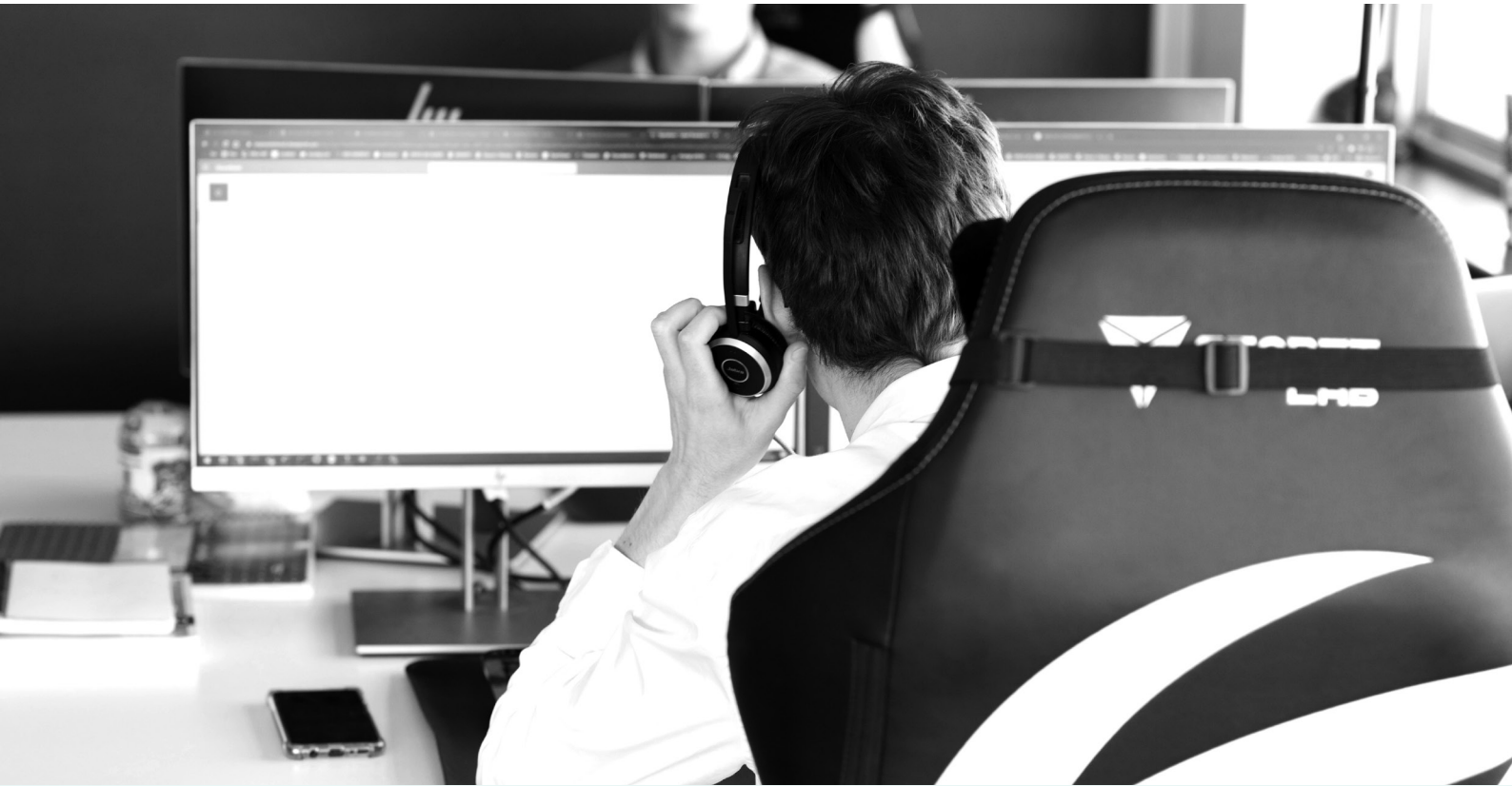


Building a Disaster Recovery Plan: Five steps to success



Building a Disaster Recovery Plan



Introduction

Disasters can strike at any time, and they can have devastating impact on businesses of all sizes and sectors. Whether it is a fire, cyber attack, power outage, or a human error, a disaster can disrupt your business operations, damage your reputation, and cause heavy financial losses.

In this guide, we will outline five steps to building a Disaster Recovery Plan (DRP) that will allow you business to plan for a minor data loss or power outage as well as recover from a larger systems loss. We will start with assessing your IT needs and risks, then go through each step right through to testing and updating your plan.

Step 1: Conduct a Business Impact Analysis

The first step to building a DRP is to conduct a business impact analysis (BIA), which is a process of identifying and evaluating the potential effects of a disaster on your business functions and processes. Think of it like a health check of your systems which will help to answer these questions:

- What are the critical systems and data that support your business operations each day? Think of each person's/team role in the business and what they could not operate without on a daily basis.

Building a Disaster Recovery Plan

- How quickly would you and your team need to regain access to systems – your recovery time objective (RTO) and is there a priority/order for which systems would be needed?
- How far back would you need to be able to recover your data – your recovery point objective (RPO)? For example, if you had a system failure at 1pm would restoring to a backup from 6pm the previous day be acceptable? or would you
- How much data does your business need to store? If you lost data would you need to access an archive which showed a file from a year ago?
- What are the potential threats and vulnerabilities that could affect your IT systems and data? If you have a risk register you can start by referring to this and then work with your IT department or IT support provider to check if anything else should be considered in your plan.
- What are the financial and non-financial impacts of a disaster on your business, such as lost revenue, customer dissatisfaction, regulatory fines, or legal liabilities? This will inform your business on the potential cost of no action versus the cost of improving security, back up and



A BIA can help you prioritise your IT systems and data based on their importance to your business and the urgency with which your colleagues would need access. This will allow you to determine the appropriate level of protection and recovery for each system/store of data.

Step 2: Develop a Recovery Strategy

The second step to building a DRP is to develop a recovery strategy, which is a plan of action that specifies how you will restore your IT systems and data in the event of a disaster. A recovery strategy should answer these questions:

- Who will be responsible for the DRP? Who will be on the disaster recovery team and what will their responsibilities be? A disaster recovery team would normally include the business manager, IT manager, and the security manager.
- What are the communication channels and protocols that will be used to notify and coordinate the disaster recovery team and other stakeholders, such as employees,



Critical Systems may not only include IT Systems, but also buildings, machinery, vehicles and people.



Building a Disaster Recovery Plan

customers, vendors, or regulators?

- What are the backup and restoration methods and tools that will be used to safeguard and recover your IT systems and data, such as cloud backup, offsite backup, or backup software?
- What preventative measures could be used to protect systems, such as enhanced security, training, and safety equipment?
- Are there any alternative IT resources and facilities that will be used to resume your business operations, such as cloud computing, virtualisation, or co-location?

A recovery strategy can help you define and document the steps and resources that are required to achieve your recovery objectives and resume your business operations as quickly and smoothly as possible.



The plan shouldn't just involve IT and senior management. Other staff may be included to assist with things like internal and external communications, making resources available and admin.



Step 3: Create a Recovery Plan

The third step to building a DRP is to create a recovery plan, which is a detailed document that outlines the specific actions and procedures that will be executed in the event of a disaster. A recovery plan can help you answer these questions:

- What are the triggers and criteria that will activate the DRP, such as the type, severity, and duration of the disaster? Who can trigger the DRP?
- Do you know what information your insurance provider would need and when you should call them? Does the DRP team know the ref. and how to contact them?
- What are the phases and tasks that will be performed during the disaster recovery process, such as the preparation, response, recovery, and restoration phases? Who will be responsible for each phase/task? In the event of a data loss or cyber attack it is important to liaise with your IT support provider to know what to do/not to do.
- What are the checklists and guidelines that will be followed by the disaster recovery team and other stakeholders, such as the backup and restoration procedures, the communication protocols, or the security measures?
- What are the resources and tools that will be used during the disaster recovery process, such as your IT support provider, your backup and restoration software, communication devices, or emergency kits?

A recovery plan can help you organise and document the actions and procedures that are necessary to implement your recovery strategy, restore your IT systems and data, and get

Building a Disaster Recovery Plan

everyone working again as quickly as possible.



The recovery plan should be available off-line and off-site in case IT systems are not available, for example on a USB stick or printed.



Step 4: Test and Validate the Plan

The fourth step to building a DRP is to test and validate the plan, which is a process of verifying and evaluating the effectiveness and readiness of your DRP. Testing and validating the plan can help check that your initial objectives have been met and that recovery tools meet your requirements:

- Does the plan meet your recovery objectives, such as the RTO and the RPO?
- Does the plan cover all the possible scenarios and contingencies that could occur during a disaster?
- Does the plan align with your business needs and expectations, such as the service level agreements (SLAs), the compliance requirements, or the customer satisfaction?
- Does the plan have any gaps, errors, or weaknesses that need to be addressed or improved?

Testing and validating the plan can help you identify and resolve any issues or shortcomings that could affect your disaster recovery performance and outcome. You can use various methods and techniques to test and validate your plan, such as tabletop exercises, simulation tests, or full-scale tests.



Tabletop exercises are a good way to share and test your plan.



Building a Disaster Recovery Plan

Step 5: Update, Maintain, and Communicate the Plan

The fifth and final step to building a DRP is to update, maintain, and communicate the plan, which is a process of reviewing, revising, and sharing your DRP on a regular basis. Updating, maintaining, and communicating the plan can help you answer these questions:

- Have there been any changes or developments in your business environment, such as new IT systems, new business processes, new regulations, or new threats?
- Have there been any feedback or lessons learned from your disaster recovery tests or actual incidents, such as best practices, improvement suggestions, or corrective actions?
- Have there been any gaps or discrepancies between your plan and your actual performance, such as outdated information, missing procedures, or insufficient resources?
- Have you informed and educated your disaster recovery team and other stakeholders about your plan, such as the objectives, responsibilities, procedures, and resources?

Updating, maintaining, and communicating the plan can help you ensure that your DRP is current, relevant, and effective. You can use various tools and techniques to update, maintain, and communicate your plan, such as audits, reviews, surveys, or training sessions.



The plan should be made available for everyone who will play a part in it.



Conclusion

Building a DRP is a vital and challenging task for any business that relies on IT systems and data. It requires a systematic and comprehensive approach that involves assessing, developing, creating, testing, and updating your plan.

TechWyse has been assisting business with their IT business continuity for over 20 years, and can assist in protecting your IT systems and advise on building a DRP that matches the needs of your business.



**If you have more questions about
IT support or disaster recovery, or
need some IT advice, give us a call
or send us an email.**

**03332 400 660
info@techwyse.co.uk**