NODE4

Empowering business to do more

Maintaining Business Continuity: Potential Disasters and How to Prepare for Them

WPMBC21

Introduction

Business continuity and disaster recovery come into play when the event you thought might never happen to your organisation, happens. Such events can vary wildly in terms of their nature, the level of control you have over them and their impact on your business – from ransomware attacks to extreme weather conditions to health incidents such as the Covid-19 pandemic.

While some events seem extremely unlikely, if they pose a reasonable risk to your organisation, you need to be thinking about them, documenting plans and testing out those plans. Disasters, in all shapes and sizes, can have a huge impact on your productivity, your reputation and affect the things that count towards the future of your business – customer satisfaction, shareholder confidence, revenue and so on. In a worst-case scenario, a disaster can mean your organisation closes its doors for good.

There may also be consequences you've not fully considered. A **2020 BCI Horizon Scan Report** found that negative impact on staff morale/ wellbeing was the second most frequently cited consequence of disruption, with 42% of organisations reporting this ahead of financial impact.

The reality is that disasters can massively affect your workforce, how it feels towards your senior leadership team and its productivity. Cracks start to appear when organisations focus on managing a crisis externally, without clear communication and reassurance to staff.

In this paper, we consider the disasters that most businesses are talking about and that your organisation needs to consider as part of your Business Impact Analysis. We then highlight technologies and best practices that help you get into the best possible shape and minimise the consequences discussed above.

Business continuity vs disaster recovery

Business continuity focuses on keeping your business running during a disaster, and disaster recovery forms a part of this. Disaster recovery is all about restoring access to your data, IT infrastructure and services.

The Disasters That Businesses Are Talking About

Unfortunately, there's not a catch-all list of disasters you can prepare for. The kinds of disasters you'll be discussing in the board room will very much depend on your organisation. If your office was originally built on a flood plain, climate change over recent decades means you'll need to factor the risk of flooding into your business continuity plan. If you're handling financial information that must never get into the wrong hands (think pension records, National Insurance records, etc.), you'll be taking the reasonable precautions that other organisations take, as well as considering more unlikely scenarios such as political upheaval.

There are, however, some common themes that we're discussing with our customers, which are also highlighted as anticipated risks and threats in the next 12 months in the **2020 BCI Horizon Scan Report.**

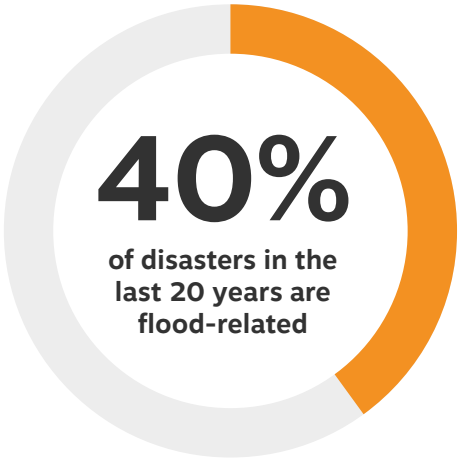
Cyber attacks and data breaches

While organisations have knuckled down on their security efforts, the hackers just keep on coming. **Forbes** reports that malware attacks increased by a staggering 358% and ransomware by 435% in 2020 compared to 2019.

When we're talking about types of attacks that lead to disaster, ransomware is the most common culprit. At user level, it can stop key staff from accessing mission-critical information, while at infrastructure level, it can perpetuate throughout the network, shutting down various machines. With staff unable to access systems, they're no longer able to do their jobs - an attack on your infrastructure, which is equivalent to someone coming into your office and smashing up your computers.

Other types of cyber attacks are less likely to be classified as disasters, unless they have spiralled out of control and you no longer have access to your network, mission-critical applications or offices. More often than not, there will be indications that your business has been compromised, but it's still able to function. In this case, rather than rolling out your disaster recovery plan, you'll turn to incident response, which is more about investigation and less about reacting to an immediate disaster.

Extreme weather



UN researchers claim that the first 20 years of this century have seen a staggering rise in climate-related disasters. According to their research, floods have accounted for more than 40% of disasters, storms 28%, earthquakes 8% and extreme temperatures 6%.

Even if earthquakes are low down on your list of concerns, the rise in global average temperature when compared to the pre-industrial period means more frequent heatwaves, droughts, flooding and winter storms.

An unseasonably hot day could overload the cooling systems in your server room, leading to servers crashing and resulting in downtime. On the other hand, a sudden cold snap may bring down powerlines, leaving you in the midst of a power outage. Either way, you must be prepared for more unpredictable weather.

> **The average cost per regulatory disruption in 2020 was £1.71m**

Regulatory change

According to the **BCI Horizon 2020 Scan Report,** regulatory changes cost the most per incident (to the eye-watering sum of £1.71m per incident).

While financial services companies are most likely to be hit by this category of disruption, other sectors are not exempt. For UK organisations spanning various industries, Brexit and legislative 'loose ends' are a big concern. The main issue is the UK being a 'third country', which means personal data cannot be easily transferred between Britain and Europe.

The hope is that the EU will grant the UK 'data adequacy', allowing data flow across the EU to continue. Unfortunately, organisations don't have a crystal ball to predict the decision-making of the EU, so many are looking at how they can prepare for the possible outcome. Preparatory measures include moving offshore data into onshore (UK) data centres and doing supplier due diligence. Ensuring suppliers comply with ISO 27001 and PCI DSS is a must for those who want to have a level of control over processing, storing and transferring data securely.

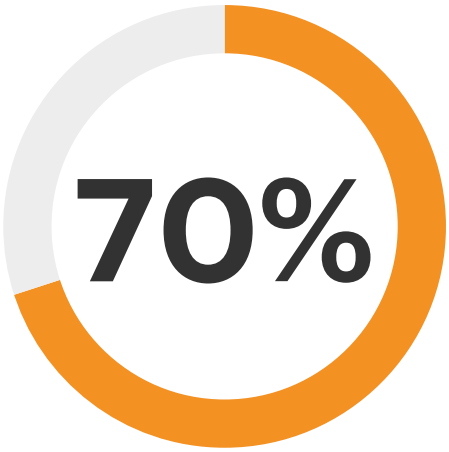
Lack of talent and skills

According to a **Microsoft report**, 69% of UK leaders surveyed believed their organisation has a digital skills gap in 2020, with 70% expecting to experience one in 2021. Digital capabilities are needed across industries and departments, not just within traditional 'tech' roles or the IT department. In fact, **LinkedIn's Economic Graph** shows that between December 2020 – February 2021, top trending skills across all UK industries included JavaScript, digital marketing and data analysis.

Though faced with skills gaps, many organisations can't just sit and wait for them to be filled. To minimise costs and keep up with competitors, you need to deploy cloud-based applications, many of which are on new, containerised platforms. The risk comes in when your staff are working with technologies they've not used before. The IT team might be able to deploy that new application, but do they know how to back it up and protect the environments?

When it comes to new technologies like Artificial Intelligence and the Internet of Things (IoT), you can be so dazzled by the possibilities and so under pressure to keep up with competitors that you fail to understand them properly and ratify them through change control.

For example, you might introduce IoT to log staff movements around the office. This results in some valuable insights for facilities management, but the sheer amount of data could flood the network, slowing down transactions with customers.



of UK leaders expect to experience a digital skills gap in 2021

Getting Your Technology Right

When a disaster hits and all else fails, you need a technology solution that enables you to restore access to your data, IT infrastructure and services. Depending on your requirements, you can rely on backup or disaster recovery (DR) solutions or a combination of the two. Here we outline the differences:

Backup

Backup means taking a complete copy of your data at one point in time. It's common for organisations to perform full backups at least every 24 hours supplemented by snapshots on a regular basis (hourly or even more frequently) along with retention of weekly or monthly backups for extended periods. Frequency of backups will determine the extent of data loss in a disaster. While backup isn't always ideal for disaster recovery, it is all about long-term data protection, which is why many organisations consider it alongside DR.

Pros

Cost – there are various backup solutions on the market to suit a range of requirements and budgets. These range from portable disks for small businesses that need to back up limited amounts of data, to more comprehensive Backup as a Service (BaaS) offerings, where Managed Service Providers support businesses by keeping their data safe and recoverable.

Long-term protection – backup offers a different kind of protection that's attractive even to organisations taking DR solutions. Imagine you're hit with a ransomware attack; DR's regular data replication means that the malicious software is copied across to your other site. Backup enables you to go back in time before the ransomware attack and override it as if it never existed. The same goes for individual recoveries. Let's say someone in Finance accidentally deleted an important spreadsheet that was being worked on last week. Backup allows you to rewind the clock and recover that data.

Compliance – another reason why organisations who take DR might also take up backups is that they're necessary for compliance reasons (e.g. 7-year retention of financial data). When it comes to customer complaints and legal disputes, they also enable organisations to go back through their records and recover necessary information.

Cons

Data loss – when recovering data after a disaster, backups can often fall short. If you only take one backup per day, for example, you could potentially lose a day's worth of transactions, and then you'll have to dedicate resource to re-entering those lost transactions into your systems.

Long recovery times – recovery times for backups can be huge. Even if your organisation has a dedicated DR location and a host of servers ready and waiting to accept data, it could take many hours or even days to complete large data restores. Without access to the latest business data, your teams' productivity suffers and this, in turn, affects customer relationships and your bottom line.

"Backup solutions range from portable disks to Backup as a Service (BaaS) offerings, where Managed Services Providers support businesses by keeping their data safe and recoverable."

South Yorkshire Housing Association

COME HOME

Case Study - South Yorkshire Housing Association

South Yorkshire Housing Association (SYHA) wanted to ensure its critical services continue to provide help to those who need it, without wasting valuable funds. It decided to accelerate its digital transformation process with a range of solutions from one Managed Services Provider – Node4. The service wrap included backup and disaster recovery solutions.

Previously, SYHA had a contract in place that didn't cover 100% of its systems and it had at best only one to seven days of backups. With Node4, it has had 100% successful backup rate and can easily add or take out systems.

Additionally, it's been able to perform its first successful DR tests as a business. Before Node4, the test was treated more as a box-ticking exercise and was sub-par to the organisation's standards. Now, in the case of a disaster, it has confidence that it will be able to recover quickly, easily and thoroughly.

> If something happens like your building catches fire, some Managed Services Providers will not only restore your data, but also provide office space and computers from which to access it.

Disaster recovery

Disaster recovery (DR) can also be thought of as data replication or continuous backup. When you store data in one location, you store data somewhere else at the same time. It does what it says on the tin; it's ideal for mitigating business disruption arising from IT or environmental outages. Disaster Recovery as a Service (DRaaS) solutions can be pretty comprehensive, not simply providing data replication but tailored design and testing too. Some Managed Services Providers (MSP) also cater for the physical/computing element of DR. Say if your building catches fire, the MSP will not only restore your data, but also provide office space and computers from which to access it.

Pros

Reduced Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) – near synchronous data replication and virtual workload failover means you can recover your data and be up and running again in hours (or even minutes). You're less likely to achieve this with traditional backups.

A dress rehearsal – one great feature of a DR solution is it gives you the ability to test your DR plan and technology. This is achieved by periodically performing a scheduled failover of the replicated virtual environments to a sandbox environment. You can test the protected workloads without impacting production environments, and it gives you peace of mind that your end-to-end disaster recovery process works as expected. While it's possible to test your backups, who knows at what point in the cycle a disaster will occur and how much data you'll lose?

Cons

Cost – the data copying aspect of a DR solution is understandably more expensive. Typically, DR involves transmitting a lot of data across a network connection to another site at high speed to remain up to date. For some organisations, the cost of having a DR solution will outweigh the cost of being out of production for several hours or days if a disaster occurs.

The verdict

Whether backup, disaster recovery or both are best really depends on the nature of your organisation. If every second that passes is a lost sale and you need to guarantee consistently low RPOs and RTOs, then a DR solution is for you. You will, however, want to consider this alongside backup for the long-term recovery of data and compliance.

On the other hand, if your production cycles are longer and you do not need to be up and running again in minutes, hours or even a day, you can rely on a robust backup strategy. The deciding factor is often cost, i.e. when having a DR solution becomes more expensive than being out of production in the event of a disaster.

benendenhealth

Case Study - Benenden Health

Private healthcare provider, Benenden Health, wanted to ensure its critical infrastructure was DR capable. Handling sensitive patient data meant that it also wanted to work with a highly accredited and fully secure Managed Services Provider, so it turned to Node4.

The initial DR failover tests conducted by Benenden Health and Node4 offered a major step change when compared to its previous provider. Tests showed that the failover can take less than five minutes to a Northampton DR site, with Node4 looking to reduce this further as the solution is refined.

"As we move into a cloud driven approach, it is reassuring to know that we have a fully scalable platform that will support our digital transformation initiatives, ensuring that our members are provided with a modernised and always-on experience."
Chris Mullins, Head of IT at Benenden Health.

“When a disaster strikes, you want to be able to make quick decisions and act, rather than feel uncertain and lack confidence in your solution.”

What to Look for When Choosing Your Technology Solution

When you're shopping around for a DR or backup solution, there are a few basic questions you should ask before you sign on the dotted line.

Is it easy to use?

It's important your IT team absorbs every element of the solution and feels completely confident using it. It's better to have a product with fewer features that your team can use than go for a very sophisticated product that your team won't use or test effectively. When a disaster strikes, you want to be able to make quick decisions and act, rather than feel uncertain and lack confidence in your solution.

Is it easy to test?

The biggest sin any organisation can commit is not to test their DR plan, part of which involves testing a DR or backup solution. If you don't test your solution (and test regularly as your business changes), how do you know it works? If you're taking Disaster Recovery as a Service (DRaaS), look for a Managed Services Provider that builds in tests with your team.

Does it have broad availability?

With backup, in particular, you'll want to ensure that the solution you choose consistently backs up data across different environments. This is especially relevant if you're a larger organisation using various operating systems – Windows, IBM, Linux, HP and so on.

Further considerations when preparing for disasters

Beyond backup and disaster recovery, there are other technologies that could aid your organisation in a disaster. The obvious one is **public cloud services offered by hyperscalers like Azure, AWS and Google.**

If a disaster affects your IT infrastructure and services, you may find that having your data in a publicly accessible environment enables you to move faster with your business continuity plans.

Beyond technology, there are some best practices that all organisations should have in place to prepare for disasters:

A business continuity (BC) plan

This is a roadmap for continuing business operations and restoring mission-critical functions during or after a disaster. It can include (or reference) your Disaster Recovery plan, but it should focus on the continuity of the entire organisation. This means defining emergency contacts across the organisation, your backup power arrangements, alternative sites for operation, essential equipment and an alternative communication strategy if your phones and internet are down.

A disaster recovery (DR) plan

This focuses on restoring IT infrastructure and operations after a crisis. Your DR plan might reference an incident response plan for cyber attacks that cause disruption, but don't stop you from doing businesses. All businesses should have DR plans which consider potential disasters, are written down and circulated to key personnel.

A testing strategy

It's no good just thinking about disasters and documenting your intended actions. You also need to test your plans to see if they work, identify gaps and improve on them.

Test at least twice a year, perhaps more often depending on your type of organisation, staff turnover, and the number of business processes and IT changes that have occurred since the last round of testing. There are various types of test, including:

- **Tabletop exercises** – reading through the plan to identify gaps.
- **Structured walk-throughs** – taking a scenario and asking each BC team member to role-play their responsibilities. Test multiple scenarios so you know you can recover from different types of disaster.
- **Simulation** – simulating an actual disaster with the necessary equipment, technologies and staff. Unlike the other types of test, you don't look for gaps as the simulated disaster unfolds; you see it through to its conclusion and review it at the end.

Staff training

There are some disasters you have slightly more control over, such as ransomware attacks and skills gaps. While you can't stop a hacker from targeting you, you can train your staff to recognise phishing emails through for, example, online training and phishing tests. Closing skills gaps could involve enhancing your learning and development programme or sourcing training and support from a Managed Services Provider who can share knowledge with your internal teams.

Conclusion

There are plenty of angles to consider when it comes to preparing for potential disasters.

What are the most pertinent disasters for your organisation; those most likely and those that will have biggest impact on your activities?

Which technology solutions are most suited to your business needs? Do you need to get back up and running within minutes of a disaster or is it more important that your restore as much of your data as possible in the most cost-effective way?

There are also the physical and human aspects of the disaster to consider. What are your provisions for alternative sites, for example?

Fortunately, you don't have to answer these questions alone. By working with a trusted provider, you can create a more robust disaster recovery strategy, choose the right technology solutions to recover your IT infrastructure and services, and even implement security tests and training to reduce the chances of cyber attacks.

Get in touch

Want to talk through your approach to disaster recovery? We'd love to hear from you and see how we can empower your organisation to do more.

Call: 0845 1232222
Email: sales@node4.co.uk
Website: node4.co.uk/contact

WPMBC21

Node4 Ltd Registered in England No. 04759927 VAT: 192 2491 01
Registered Address: Millennium Way, Pride Park, Derby DE24 8HZ
T: 0345123 2222 **E:** info@node4.co.uk
www.node4.co.uk