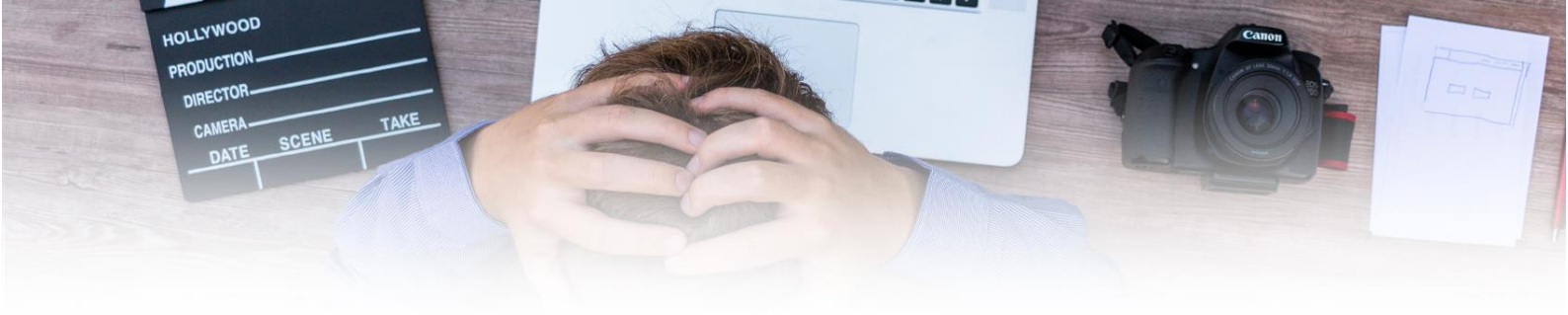
BUSINESS CONTINUITY PLANNING

"ALWAYS BE PREPARED!"

Norfolk Computer Services



SUMMARY

Business downtime can be disastrous. Working with a managed service provider, your business can prepare for the worst. For one, cloud-based backups drive an efficient returning to business as usual. This ebook examines what disasters might happen and all that a business continuity plan can offer.

“Always be prepared” is a familiar saying for Scouts. These true words can also be a business mantra. Hardware failure, security breaches, or even natural disasters are all possible. So, most businesses understand the importance of backing up data and systems. Yet, without business continuity planning, recovery is challenging.

A managed service provider plans for, and supports, your return to business as usual.

Why You Need a Business Continuity Plan

Business continuity planning (BCP) prepares your business to recover after a disaster. It's about anticipating the worst, predicting impacts, and planning to recover quickly, smoothly.

Thorough business continuity preparations consider staffing, equipment, physical premises, hardware, and software. After all, disruptions to any of these can cost your business money. Your business may:

- Lose revenues
- Need to pay extra expenses
- Encounter fines
- See profits drop
- Experience customer churn

It pays to think about business continuity in advance. You may be calm and collected in a crisis. Good for you! Still, you're likely to think more clearly if you're not in the midst of a chaotic situation. Working with a Managed Service Provider (MSP) can help too.

Have You Thought About What Happens When...

Business may be going great. You've read about other businesses being hacked. You've wondered idly what you might do if a tornado touched down and took your business out. But, nothing like that has happened to you! So, you've haven't actually made a disaster readiness plan.

Start by brainstorming all the business elements a disaster could impact. Your IT Managed Service Provider will bring together business stakeholders to run through different scenarios. For example, what will you do if:

- You are victim of a data breach or ransomware attack?
- One or more vital systems doesn't work?
- Your employees can't access your building?
- Your business loses power due to a severe weather event?
- Disgruntled employees sabotage your systems?

Even a few days downtime can be crippling. BCP also gets you thinking about:

- Whether your staff can work effectively from another location?
- Can their phones redirect to another location?
- Will they be able to access their desktops virtually?
- Can people continue to provide quality customer service or interact with vendors?

The MSP will ask these questions and more during their BCP as they:

- Analyze business impact
- Identify critical business functions and processes
- Organize a response
- Run training and testing exercises

You may be reluctant to run your business continuity team through their paces. Won't that be disruptive to business? The MSP will work to minimize interruptions. After all, it isn't enough to think about being prepared. Running tests will also help you re-evaluate your BCP choices and priorities. This is the ticket to ensuring you have the best plan in place — before something actually does go wrong.

Recovery Strategies in Real Life

You can keep your fingers crossed that you'll never need your business continuity plans. You can hope only one small part of your business systems will go down. But, you're best off planning for a massive hit. You'll be glad you did.

You may already have a plan in place to back up data. But, do you have a plan for accessing that data and getting back up and running after a disaster? What if your data in only available on local devices and the building has burned down?

You want to have more than one backup location. We endorse the 3-2-1 backup strategy. This calls for at least three data copies. Two are local (on separate devices). The other is offsite.

Still, businesses that backup their data offsite, on tape or cloned hard drives, may lose data. It's a question of how much time has elapsed since the last backup. Sometimes this is a few hours. But it could be days — costly days.

Business continuity planning will consider how often the data is created. Frequently changing data needs regular backing up. For example, a transactions database, generating hundreds of records hourly, needs frequent backup. But tax information from five years ago doesn't change much. So, it won't need backing up as often.

Since the backup is offsite, plan also to check regularly that it's up-to-date. You don't want to experience data loss and then find out your data can't be restored after all. Keep in mind too, tape or hard drive backups can be expensive and are more easily stolen. all. Keep in mind too, tape or hard drive backups can be expensive and are more easily stolen.

One more thing, don’t think that cloud storage works as backup. Services such as Google Drive or Dropbox do have their uses. They provide online spaces to store data and enable collaboration. However, cloud storage isn’t intended as a backup. Why not? Data isn’t always encrypted. Many users have permission to access the files. Data can be deleted, changed, or rendered irretrievable.

Ultimately, cloud-based backup is a more comprehensive solution.

Benefits of Cloud Backup

Moving to the cloud isn't for every business. Still, it's often a good solution for business continuity. With cloud solutions, your business can quickly restore lost data — anytime, anywhere. If something does happen on your physical premises, your data remains safe in the cloud.

Minimizing business disruptions, a cloud-based backup solution lets staff continue working from anywhere. Employees can still access data and applications working from home or a temporary office.

Cloud backup typically has file versioning in place to make it easy to retrieve files. Even previous or deleted versions of files can be accessed. Note: ask your provider about the time-window for recovering previous or deleted versions.

With cloud-based software and cloud backup, teams can continue file collaborations without disruption. A tool such as Office 365, lets users access email, calendars, and files in real time, wherever they're working. Files sent to the cloud are encrypted, so you don't have to worry about security either. The cloud-based backup provider isn't actually ever seeing raw data. This also makes cloud-based backup a cost-effective compliance safeguard.

Partnering with a cloud-service provider you gain experienced support. Working with an MSP, you gain top cloud technology and peace of mind you're ready if something does go wrong.

Maybe they'll want to mess with your IT infrastructure and shut you down. Imagine a denial of service attack as a bug infestation that is so constant you are driven from your home. With the boom in cryptocurrencies, some bad actors want to leverage your computers' processing

power. You'd eventually notice your computers running slower and skyrocketing utility bills.

Key Takeaway

Planning ahead can help your business get back to normal efficiently if disaster strikes. An MSP can lead your business continuity planning and help you determine if the cloud is right for you.

Disaster can strike any business, of any size. Don't wait until it's too late to approach a managed service provider. Ensure your business survives, no matter what happens.

Call us at 01953 857980!

Norfolk Computer Services

Hethel Engineering Centre
Chapman Way
Hethel
Norwich NR14 8FB

Phone: **01953 857980**
Email: **enquiries@norfolkcs.co.uk**

Web: www.norfolkcs.co.uk
Facebook: facebook.com/norfolkcs