

Brought to you by



**SOUTHERN IT**  
N E T W O R K S

# YOUR 25 POINT DATA DISASTER CHECKLIST

SEE HOW PREPARED YOUR BUSINESS  
REALLY IS WHEN DISASTER STRIKES

---



**SOUTHERN IT**  
N E T W O R K S

[www.SouthernIT.com](http://www.SouthernIT.com) 01323 287828



# DISASTERS HAPPEN... EVEN TO YOU

*It's your responsibility to make sure your business, and its data is safe, secured and available in the event of a disaster.*

It's no secret that many small business, and some not so small, suffer as a result of data loss. It is well publicised when the media get hold of it, because quite frankly it's irresponsible and un-necessary these days.

Business failure is not so sensational for the media but far more painful for you, the business owner or IT manager, who has to deal with the fallout.

“

What our clients say:

*“Southern IT came on board as our IT provider 4 months ago and don't know how we survived without them before!”*

*John Jones, Managing Director,  
Bexhill Electrical Ltd*



# DISASTERS COME IN ALL SHAPES AND SIZES

*If you are not sure if your data is protected, or if you can recover it quickly (or not at all), run through the 25 points we have found to be the most critical for small business like you.*

The storms and flooding during the winter of 2015/16 have been devastating for home owners and businesses alike. None had any warning and only realised how ill prepared they were when it was too late. How would you feel if you were one of these business owners? Business failure is not so sensational for the media but far more painful for you, the business owner or IT manager, who has to deal with the fallout.

But scaremongering aside, there are some simple things you can do to ensure you are protected when disaster strikes your business.

This document is not intended to detail all of the possible disasters you may face, they are far too many.

However, this checklist will help you look at your data management in a more structured way and will help you consider measures that will help manage most disasters.



# YOUR ABILITY TO DEAL WITH A DISASTER

It will only take a few minutes and there is no technical geekery involved, just plain business related questions.

Each section approaches a different area and will ask questions you may not have considered before. Each has a short description that will help you understand the relevance and impact to your business.

Score yourself honestly on each answer and at the end of the checklist you will see where you are in each area.

Once you have been through this on your own, go through it with your IT person, it may help to clarify some of the points you are not aware of or not exposed to.

If you outsource your IT, or just your data backup, this will help to establish if your IT supplier has you covered for all eventualities. Use the questions next time you review your contract and see how easily they answer.

We hope this helps you manage your IT more easily, it & certainly something we do every time we meet with a new customer so we know how useful it is.

## TAKE THE TEST

Take a few minutes to answer our questions and see if you can manage your IT more easily.

***Continue to Start our 25 point checklist...***



# THE CHECKLIST IS SPLIT INTO THREE LOGICAL AREAS:



## *How well is your business protected*

Knowing you are protected and how is fundamental to protecting your business when (and its not an 'if') disaster strikes. Disasters come in all shapes and sizes. From a failed disk drive to a lost laptop that holds critical data all the way through to a complete business destruction, as we have seen recently due to the bad weather in the north of England.

So the first section of this checklist deals with how (and if) you are backing up efficiently.



## *Managing data backup*

Just having some data in a safe place is better than nothing but often its not enough. How you do it, what you do it with and where your data is are all crucial to your ability to recover when the worst happens.



## *Dealing with a disaster*

Having data in the right place and knowing what you have is key.

Unfortunately most businesses fall at the last hurdle. Knowing what to do and who is going to do it when everything is chaotic and stress levels are running high is the final hurdle (at least when it comes to your data!)



# HOW WELL IS YOUR BUSINESS PROTECTED

## 1 *How is backup taken care of?*

If your answer is anything but automated, you are going to fall foul of Human error at some point. Through sickness, holiday or just plain forgetfulness you will miss backups, and we all know that it will be at the time you most need your backup that it will fail.

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Don't know	In House Staff	IT Supplier	Automated

## 2 *Is data centralised?*

The more centralised data sources are, the easier they are to backup up. This isn't strictly true with newer cloud backups, but it does add to the administration overhead when backing up and restoring data.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Don't know	Some is	Most is	Yes, all centrally

## 3 *Is data in a safe off site location?*

You should have at least two geographically disperse copies of your backup, if not three. That backup on a USB drive in your office is not good if your building burns down, or get stolen. Don't fall in to the trap of it being someone's job to take the drives home each night, you're back to human failure again.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Don't know	Maybe	Highly Likely	Yes

## 4 *My backup is monitored daily to ensure it worked and is reliable*

Sometimes things just get in the way. Maybe a power outage or a file that was corrupt. There are a hundred things that can interrupt your backup. So having something in place to spot that and alert you is the first step.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
No	Maybe	In House Staff	IT Supplier



## 5 How often does your backup run?

Have you sat down with your IT Provider and worked out how much data you can afford to lose, or have you just gone with you IT providers' standard backup regime? If you could only afford to lose 4 hours' worth of data, but the backup only runs once per day then what does that mean for your business? Don't leave it until you have the event to find out!

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Don't know	When we run it	Weekly	Daily

## 6 How often are your backups tested and validated?

Put simply a backup that is not tested, is only marginally better than no backup! We don't like to be in the backup business, but the recovery business, I'm sure you'd rather have your IT provider do that also.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Don't know	When we remember	Monthly	Weekly or less

## 7 Critical data is backed up how often?

Ideally, this data being the lifeblood of your business, you should be backing this up more often than the rest of the data.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Don't know	Weekly	Daily	Every 4 Hours

## 8 I have retained data for (how long)

How long do you really need to keep your data? Some legal requirements and compliance regulations have different requirements.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Don't know	Forever	1 Year	3 Years

## 9 I review my backup policy regularly

Business changes constantly, so should your processes. Backup is just one of the areas that should be reviewed regularly so that you are protecting the right data. If you face a disaster and only discover that the latest backup doesn't cover your new accounts system.....you might find out the hard way.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Don't know	Each Year	6 Months	Each Month

Now add up the totals here to see how you did  
**HOW WELL IS YOUR BUSINESS PROTECTED**

Total.....

Continue our 25 point checklist...



# MANAGING DATA BACKUP

1

2

3

4

**10** *We use a cloud service that lets us share files and keep them offsite – but what data is backed up separately?*

Unfortunately many of these solutions are not providing you with a backup, just a centralised share. Even with versioning on something like Dropbox there is no guarantee that your all data can be recovered. Even if all of your current user data is in a file-Sync your applications, programs and legacy data may will not be



Don't know



Some Data



Most Data



All of it

**11** *My data backup is completely secured and encrypted so that no one other than my trusted staff can access it.*

Don't forget, encryption keys are held by you. Your supplier should not have access to these and only trusted staff should know what they are. If you lose the keys (forget the pass phrase) no one can get your data back.



No



Maybe



Highly Likely



Yes

**12** *My data backup is stored where. Do you know where and what situation?*

Are you sure your data is secure and available? Many online services will not guarantee your data is in the UK for example. That might mean you face exposure if you are storing sensitive or personal details.



Don't know



Maybe



Highly Likely



Yes



**13** *The backup contains data that has been selected according to importance we were consulted on what this contains*

Do you know what is in each backup job and why? Many online backup solutions will just default to specific folders on a computer or server. If you do not know which these are you might find that your critical data is not being backed up, at all.

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
No	Maybe	Highly Likely	Yes

**14** *I know which data sets are critical to my business*

There are lots of different types of data, sensitive data that only business owners and directors should see, general data, legacy data and lots more. Each set needs treating differently.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
No	Maybe	Highly Likely	Yes

**15** *Non-essential data is backed up as part of my regular jobs?*

Backup might not be the most cost effective way to save the non-essential data. Perhaps archiving is more relevant?

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
No	Maybe	Highly Likely	Yes

**16** *Someone checks our backup*

Checking that jobs run and are confirmed should be a regular task. Either for nominated internal staff or IT suppliers.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
No	In House Staff	IT Supplier	Automated



### 17 *Someone does a test restore of our data*

Do you know what is in each backup job and why? Many online backup solutions will just default to specific folders on a computer or server. If you do not know which these are you might find that your critical data is not being backed up, at all.

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
No	Maybe	In House	IT Supplier

Now add up the totals here to see how you did

#### MANAGING DATA BACKUP

Total.....

Continue our 25 point checklist...

## DEALING WITH A DISASTER

### 18 *If there is a disaster which means we cannot work from our office, everyone knows what to do to ensure we keep our customers serviced*

Key services and staff are all provisioned for and everyone knows what needs to happen to keep your business online and customers serviced.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
No	Maybe	Highly Likely	Yes

### 19 *If there is a fire at our office and we lose everything, we can be up and running again*

Do you have an alternative location and critical services, data and equipment to quickly bring up your business if you have to?

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
No	Maybe	Highly Likely	Yes



**20** *We have a written disaster recovery process for my data so that anyone can deal with this in a critical situation*

If data needs to be recovered in an emergency or if an IT guru isn't around how will your staff deal with it? Written processes can really help keep your business functioning and there is nothing more important than having access to your data.

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
No	Maybe	Highly Likely	Yes

**21** *We have a written disaster recovery process for my IT function so that I can not only get my data back, but I can use it immediately*

Is it just your data that is backed up? If you don't have access to the applications/ programs you need to use the data you might be in the same boat as if you had no data.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
No	Maybe	Highly Likely	Yes

**22** *There is a process in place to immediately rectify a failed or compromised backup*

Second is knowing what to do to rectify it. Have you got a documented process and the right people trained to deal with it? At the very least you should have an emergency contact list with each of your senior staff in case key people are not available immediately.

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
No	Maybe	Highly Likely	Yes



### **23** *When the worst happens we have someone on standby to help*

Making sure you have the right people in place to help with a disaster is essential. But knowing exactly what they can/will do for you is arguably more important. The last thing you need is a burned out building and an IT supplier saying 'yes we have your data, but where do you want us to restore it to?'

1	2	3	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
No	Maybe	Highly Likely	Yes

### **24** *We can easily keep the business running by working from home*

With a reasonable internet connection at home you and your key staff can operate from remote offices. Often it is not the location that causes the problem, are you sure you have access to all of the essential programs, applications and data?

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
No	Maybe	Highly Likely	Yes

### **25** *We test our disaster recovery process*

Businesses evolve and grow so the processes you operate should be developed to suit your evolution. But how often do you make sure they are?

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Never	Each Year	6 Months	3 Months

*Now add up the totals here to see how you did*

#### **DEALING WITH A DISASTER**

Total.....

*Continue to see your performance review from the 25 point checklist...*



# YOUR PERFORMANCE REVIEW

After answering all of the questions in this checklist you will probably have had to do a little searching or asking for information.

Hopefully that has helped you identify areas where your business could tighten up and be more efficient.

*Now it's time to see how your business rates in terms of data backup.  
Add up the totals for each page here.*

## HOW WELL IS YOUR DATA PROTECTED

Total.....

## MANAGING DATA BACKUP

Total.....

## DEALING WITH A DISASTER

Total.....

## OVERALL SCORE

Total..... /100

*What we have found is that business fall into four general groups based on these scores.*



## **25 or Below**

You really need to look at your data backup. It maybe that you have passed ownership of this to someone else and don't know exactly what is happening or maybe you just didn't realise some of the implications.

That's good!

Now you know some of the areas you need to look at in more detail and can take appropriate action before its too late.

## **25 to 50**

You have some data protection in place but it needs reviewing. Use the questions where you didn't score highly and talk to your team, or your supplier, to see how these can be improved.

## **50 to 75**

We find that people in this band are reasonably well covered but drop scores due to management or processes.

Its worth taking a look at those and making sure your staff, suppliers and management all have a good understanding of what should happen when disaster strikes.

## **75 to 100**

You probably have most of this covered but there is still a gap somewhere.

It maybe that there is one area of your data backup regime that needs attention. It could be that you need to look at a more comprehensive disaster recovery plan, something that will help you deal with a disaster more efficiently.

**Whichever band you are in we hope this checklist has helped you see data backup and recovery for the critical service it is.**

**If you would like more information on data backup, recovery or disaster planning please contact us at:**

**To give Southern IT a completely risk-free try you can:**

- 1. Call me on 01323 2878288 or 07779 125855**
- 2. Email me at [Michael.Freeman@SouthernIT.com](mailto:Michael.Freeman@SouthernIT.com)**

WE CARE. ABOUT YOU.  
**YOUR BUSINESS.**  
AND YOUR SUCCESS.