

Data Backup and Disaster Recovery

IT support, even before you need it



Myths about IT that could sink or float your business- And what you can do to flourish instead

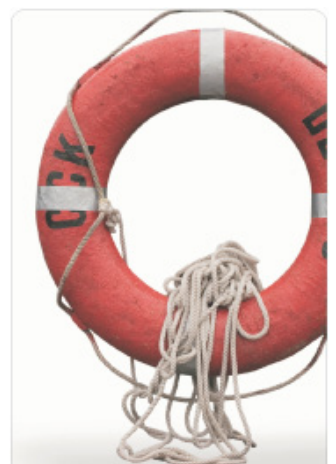
Introduction

Please blow a raspberry in my general direction if after reading this, you discover I have been overly doom-mongering. You see, if you pass the checklists, not only have you protected yourself, you are really looking after your clients by making sure your business can bounce back after even little data disasters.

Unfortunately, you are unusual if all of your data is safe.

And that's not because everyone else is somehow careless. The sad fact is, many small businesses I meet for the first time are simply unaware of how much of their data is at risk. Until that is you have felt the pain of losing some, or all of it. Shock And Horror Turns To Fear – The Reaction Of Business Owners Who Suddenly Realise How Vulnerable They Are. My worst nightmare is a client suffering a data disaster.

So when I meet a new client for a chat about what they want, I need to know how safe their data is. Sadly, our company is often recommended after a disaster. And it's usually at a point when the client hasn't realised the full extent. They may well have recovered some of




Help!

When you need it,
and before you
need it.



Abussi Ltd. provides small and medium businesses with the high level of IT support larger companies enjoy, without the high level of investment. Instead of employing an expensive in-house IT department, Abussi partners gain unlimited support from an entire staff of qualified experts. Our services include consulting, implementation, support, monitoring and maintenance of your IT systems, all for an affordable monthly rate. Our solutions will save you money, decrease downtime and allow you to focus on what matters most – your business.

 Don't wait until it's too late.

their data already. And the reason we have been recommended is because they haven't yet got all of their data back.

It's at this point that the questions I ask before any potential disaster could have saved them. The fear creeps in once they consider their position if they don't redress them. I'll give you everything you need to solve any gaps. But first, instead of giving you a jargon-filled list of technical terms which you may or may not be able to cross-check, I'll give you a list of things people have usually forgotten to cover when it's too late.

8 Common Things The Disaster-Struck Didn't Do

1. The most obvious, but amazingly still not done by many, is backing up data in the first place.


2. Frequency of back-up. If you came into your office tomorrow, and realised that a vital quotation you prepared 3 days ago had been deleted, would you be happy that your weekly back-up didn't contain it? Could you remember enough of the detail?


What if you had forgotten the week before to run your back-up? What if all of your accounts data had been lost since the last back-up?


3. Which leads me to accounts data. Sometimes people assume that because they have a network back-up facility, it covers all of their data. A very common omission I find with new clients is their accounts data. It is sometimes installed on a PC, and the accounts data is stored on that PC, and not on the network or in the back-up schedule.

4. Email. Many people don't think they need to recover their email. That is until they lose it. I'm talking about the messages that arrive in your inbox, and are sat in your "Sent items" folder.

Email communications are increasingly used as legal evidence of a contract or an instruction to proceed. Have you ever used a solicitor to represent you? Even if you haven't yet, it can cost you hundreds or

 Backing up your work doesn't have to be a chore.

 Your email is more important than you may think.

 Knowing how your system works is the first step in safe business practices.

thousands of pounds if a vital piece of email evidence cannot be produced should it be needed. Some of our clients are required by the quality assurance standards of their professions to retain all incoming and outgoing emails for a reasonable period.

5. File and folders. The converse of making sure vital data such as accounts information or emails is covered, what about the seemingly mundane? Word documents, spreadsheets, and databases are important. How important are they if they can't be recovered?


6. Storing information in the wrong place. When you hit the save button, do you know where the document is stored? Is it in a location on your PC or network that is scheduled to be backed up?


Saving your work on the desktop of your PC or in the My Documents folder isn't much use if your back-up selects data from a shared location on a network.

7. Contact and calendar information. Many people use their contact and calendar folders in Outlook or other popular email software. They don't realise that in small networks, that is stored on the PC and not backed-up unless you explicitly do so.

More commonly, in businesses with a network, it is stored on the file server. Unfortunately, their back-up software wasn't configured to back up contact and calendar folders too. Those that suffer a data disaster are often completely lost, not knowing who they were due to see, or even being able to contact them without access to the data they stored in Outlook.

8. Where your back-up is kept. Do you use pen-drives, CDs, back-up tapes or hard drives to back-up your data? Great. But where do you keep it? Next to your PC or file server? In a locked drawer? In the company safe?

 Theft isn't the only threat to your business data.

 If your office was on fire, would you be able to grab everything you need to stay afloat?

Whichever method you use, consider the worst case. A thief will just as easily pinch a back-up tape or pen-drive as they will your PC, laptop or file server. And equally, fire does not decide what to burn. Nor water what to damage. That's why the best back-up procedures become completely useless unless you regularly take your data home.


PCs, laptops and file servers can be replaced following a disaster, but your data can't. So very regularly, in fact in most cases daily, make sure someone is tasked with taking your tapes or whatever home.


Now this is not an exhaustive list. There are sometimes other pockets of data that you need to secure. The best way to think about it is to imagine what you can't live without should disaster strike. Think of the things you do on your PC each day. And question where the important data is situated. Don't worry about software – you should have the CDs for that. It's the data associated with the software that's important to protect. So if you have a piece of software, for example which helps you track your work, where is the data stored? Is it on your PC or on a shared drive? And then check whether it is part of your back-up schedule.

How IT Cowboys Put You Off Acting, Or Falsely Tell You Everything Is Okay

I hate meeting new clients who come to us in desperation following a disaster. It's a horrible situation. They are really looking for a magic-wand solution to what's just happened. And in nearly every case, the situation was avoidable. I want this document to help you avoid these mistakes. So straight away, I could be in danger of offending either somebody you employ who may not have all bases covered.

Or as is often the case, the company that advised you. Forgive me for my bluntness, but whether you like it or not, the buck stops with the owner of any small business to be responsible for, and be certain that their data is protected.

 Data protection is your responsibility.

 Take an integral part in the security of your business.

The very survival of your business depends upon it. That's why the crest-fallen small business owner, realises too late, that those few words of reassurance from their unqualified "expert" were insufficient. After all, would you be happy accepting "It's perfectly fine, I fly better when I'm drunk, the flight console does the hard work" from your pilot as he staggers into the cockpit just before take-off?

The challenge is knowing how to properly question such sweeping statements. Your expert may not be as obviously incapable as a drunken pilot so let's look at a few questions even the IT-phobic can use to be sure.

Check-list And Questions You Can Use To Make Sure Your Data Is Safe

Where is all of my important data stored?


While you may want to know exactly where for your own piece of mind, you are really questioning whether your advisor knows. Give them a quick checklist and ask them to tell you whether the following is stored on a PC or shared drive:


1. My/our accounts data
2. Our emails – inboxes, sent items folders
3. Our calendars and contact folders
4. The data associated with any software we use
5. Files and folders (Word documents, Excel spreadsheets etc)

How do you know the back up works? (&) Can you show me the screen that confirms this?

N.B.

You don't need to know how to tell, just that they are prepared to show you the screen which confirms this. After all, they don't know whether you are IT-savvy or not. But you can be worried if they avoid the the question! And if they show you, use the above check-list so you can see each piece of important data is being backed-up. Or simply assess their body-language if you wouldn't know what to look for!

 Data backup shouldn't be sporadic.

 Make data backup a part of your daily routine.

How often is my data backed-up?

Ideally, every small business should back up their data every day. While people can manually save to CDs or pen-drives each day, it can be laborious. It costs a lot less than you think to get a piece of software which will schedule this for you or a colleague to look after. The thinking has therefore been done for you, and all someone has to remember to do is remember to take the CD, tape or hard drive home each day.

Who is responsible for it?

Having your data automatically backed-up over the Internet is ideal. However, it can prove expensive. And often, there are hidden costs which the innocent should be wary of. But consider it if your data is more important than the extra cost. Like a lot of things in the IT world, prices are coming down. But until then, the most cost-effective way is to bring it in-house and do the daily back-up yourself, or nominate a colleague (and in their absence a deputy) to run through a daily routine.


A good routine will only take 2 minutes. Usually, it's just a case of changing over the tape or hard drive marked with the relevant day of the week. So if it is a Tuesday, you put the "Monday" drive in your coat pocket or hand-bag, and put in the drive marked "Tuesday."


Just make sure you have a spare in the office for the day that you or the person responsible forgets to bring in the drive from the corresponding day the previous week!

N.B.

Because people rotate tapes or hard drives, every week or so, you're over-writing the one which is 7-8 days old. So, if you deleted a file a fortnight ago, you may not notice until you need it and the tapes/drives have been over-written.

Make sure you consider archiving. You can do this weekly, fortnightly, monthly, bi-monthly, quarterly, bi-annually, or perhaps just once a year. The cost? As many tapes or drives as your budget allows. And also ask about file auditing. This is software which keeps ALL versions of a file,

 The right IT ensures you'll never forget to back up your data.

 Check your data regularly to make sure your backup plan is working.

even deleted files. Ask your IT provider about that.

What checks and balances are in place so you can be assured it is all working?

It's all very well entrusting back-up to someone in-house, but how can you legislate against them forgetting? Most good back-up software can be set to automatically email you each day to tell you and/or your support company if there was a problem. This gives you a gentle nudge each day to change the tape in case you've forgotten.

Just as importantly, it is important you test it by restoring a random file every once in a while. Again, I've come across some situations where the client thought they were doing everything right, but when it came to the crunch, they had been faithfully changing tapes or drives each day, unaware that it wasn't working. So make sure you regularly restore a file, perhaps a random Word document or email of your choosing, and see if it comes back okay.

Most support companies should do this for you as part of regular health-checks. If they don't, insist upon witnessing a test by giving them a file to restore and check that it worked to satisfy yourself.


You're Safe: So What Do You Do When Disaster Strikes?


Following September 11, we all started to hear about business continuity plans. And we may have switched off, or put it on our things-to-do list but never gotten around to it.

It's easy.

Too often, it's over-complicated by the consultants. And while it is wise to spend a little more time on it, it's better to put together at least a 1-page document than do nothing at all.

Data Backup and Disaster Recovery

 Are you prepared for the worst?


 Back up your backup plan with emergency files.


20 minutes from a smoother recovery. That's right, you can produce a continuity plan in as little as 20 minutes which will cover the basics. Consider producing a document with these elements:


- A list of staff telephone and mobile numbers as well as their postal addresses – but give everyone a copy to take home in case it is ever needed.
- Note whether they have broadband access at home – many will be able to continue working if they have. And note who keeps back-up data at home so you can get cracking on restoring the data as soon as equipment is in situ.
- A note of your email provider's user name and password so you can get to and reply to emails from somewhere other than your office.
- Get a quote for replacing all of your IT equipment, and in particular a PC or file server with everything necessary to restore your data onto. Then, you are ready to act quickly without starting the shopping process. And keep it at home with the phone numbers and contact details you will need to act.

Decide where your operation will be based

- Immediately
i.e. on the day and subsequent few days following the disaster. You may decide that working from home will be sufficient for you and your Colleagues.
- In the short-term
Beyond the first day or so, you may wish to use a temporary office, where some or all of your staff can base themselves. Look one up in the Yellow Pages and note down a few that are geographically suitable so you have their contact details in advance.

 What's your plan for disaster?

 Hope for the best, but prepare for the worst.

 Find inexpensive ways to secure your business data.

- Longer term

Consider your insurance. You may be covered for office equipment and premises, but what about loss of earnings? Or a fund to cover your immediate and short-term needs? Get those policies in place so you have a long-term future beyond the disaster, because you've bridged that immediate gap.

Nominate responsibility

This may sound a bit morbid, but depending upon the disaster you may want to delegate responsibility to one or more people. The disaster may mean that not everyone will be available to take charge.

One of the unexpected experiences of disasters like 9/11, was that the people you would naturally expect to take charge – the MD of a company perhaps - were often less effective in taking charge during a crisis.

So people you would not ordinarily expect to lead recovery in a disaster may be more suited. People with good organisational skills who are cool in stressful situations may be just as good leaders, or at the very least able deputies should the usual leaders in your business be incapacitated because of the disaster.

Shopping List – What You Need To Back-Up Your Data

Cheap and Cheerful – Home Based Businesses

Buy two USB hard drives. These can be attached to your PC to copy data to and from. Do this regularly. Daily if you can. Copy all of your important data – including accounts data, word processing and spreadsheet files, and your email/calendar/contact folders.

Some hard drives come with software which take a little of the pain out of the task. Why two drives? To cover you for fire / theft. Keep one of the drives in a different location in the home. The second drive, perhaps once a week, run an additional back-up and give it to a friend or relative to keep for you. That way, should your house burn down, you can get your data back.



Beware of online backup fees.

Also, consider on-line back-up services. While the cost often exceeds the cost of hardware and do-it-yourself back-up, it may still be relatively inexpensive.


Office-Based Businesses

There are a number of choices. While usually more expensive than having your own hardware, your budget may stretch to make online back-up services a good choice for you. Be careful though. Especially with a file server which collects and distributes your email, online services often back-up log-files which are not essential and add to your monthly bill without you noticing.

The most inexpensive way is by using tape drives or external hard drives. We are moving away from advising clients to use tape. Hard drives are inexpensive. In fact cheaper now than some of the tapes we used to recommend.

With 7 hard drives, you can use 5 to run your back-up Monday to Friday. The two spare can be used to rotate so you always have one at your or an employee's home. The other can be used to take regular archives. I would also strongly recommend you use some good network back-up software. We recommend Backup Assist, because it can manage the back-up of all email, calendar and contact folders.

It is far more reliable than some of the applications that come bundled with file servers. And it takes the drudgery out of the routine for internal staff. It should take you 2 minutes or less each day. Just swap the hard drive and the software will take care of the rest – and more importantly email you to confirm the back-up was successful.

 Rely on the professionals for the highest level of business data security.

Get Advice From An Expert

Look up a reputable IT provider for either one-off advice if you run your IT in-house. Or even to visit, conduct a data health-check, and if necessary get your data secure for you.

Ask them the questions featured in this article. Most importantly act upon it. I once heard about a company with no back up. The guy in charge is alleged to have said that if they lost all the data, there was nothing to worry about. They printed off every single document, and he had a team of typists who could re-key anything they needed.

Aside from the incredible losses they would have incurred re-typing or scanning in paper files, he forgot one important thing. Paper burns. And fires do happen. They didn't burn down, but within 6 years the company closed. Why? I don't know.

So make sure you act before it's too late.

Please Distribute This Article Freely

With preference to other small businesses you want to help, by making sure they avoid IT mistakes. Provided that the content and links are left intact, as they are, without editing and that proper credit and attributions are made to the author and his Web site.

Abussi Ltd

Craig Sharp is a director of Birmingham-based IT company Abussi Ltd.

Mailing Address

1 Victoria Square

Birmingham

West Midlands

B1 1BD

Phone: 0845 862 0200

Email: craig@abussi.co.uk

Web: www.abussi.co.uk

Legal Notice

While attempts have been made to verify the correctness and reliability of the information provided in this publication, the author and publisher do not assume any responsibilities for errors, omissions, or contradictory information contained in this document.

The author and publisher are not liable for any losses or damages whatsoever, including but not limited to loss of business, profits, service, clients, information, or any other pecuniary loss. The information contained in this document is not intended as advice, legal, medical, financial or otherwise, and provided for educational purposes only. You are highly encouraged to seek the advice of a competent professional when applicable.

The reader of this book assumes all responsibility and liability for the use of these materials and information. Craig Sharp, Abussi Ltd and all associated organisations assume no responsibility or liability whatsoever on behalf of the reader of these materials.

Additional Notice and Disclaimers

Any results depicted or implied in this document are atypical of most results. No guarantees, promises or suggestions of any results are made, whether implied or stated. Individual results may vary from those shown, and everything herein is provided on an “at your own risk” basis.

While the author has done his earnest best to make sure you enjoy this report, certain grammatical and typographical errors may still exist. Any such error, or any perceived slight of a specific person or organisation, is purely unintentional. Wherever the neuter is not used, any one gender was chosen for simplicity's sake. This document was created with the hope that the reader finds its content useful and not analysed for the purposes of gender equality, language correctness or writing style.