Crisis:

Your office is on fire

Your people are all safe... but now what?

What important preparation do you wish you had “got round to doing...?”

sedcom

Your trusted IT partner

Crisis:

Your office is on fire

Your people are all safe… but now what?

What important preparation do you wish you had "got round to doing…?"

It's the phone call no business owner or manager ever wants to receive.

A call, from the police, late at night – there's been a fire at your premises.

Luckily it was empty at the time, and no-one's been hurt at all. That's a huge relief.

You barely sleep. And at first light, you go in to examine the damage, so you can issue instructions to your staff.

The fire wasn't too big, and the fire service arrived quickly. But your premises have been utterly devastated.

The fire itself destroyed a room. Smoke has damaged the rest of the building. And it's flooded too, as a result of the firefighting.

Good thing you're well covered on insurance.

As you're surveying the damage, you see your server, located near where the fire was. It's bent and twisted – clearly that's going to need replacing.

Good thing you have a backup… no… wait… the backup…

You feel your skin go cold as you remember a conversation you had with a member of your team a few weeks ago.

They'd noticed the automated backup had stopped working. In fact it hadn't worked for some time.

You agreed a new backup needed to be put in place at some point. Till then, you asked your colleague to make a manual backup a couple of times a week onto an external hard disc drive.

That seemed an appropriate thing to do.

Where did he keep that disc?

Your eyes flick to his desk… black… charred… and dripping with water. The contents of his drawers on the floor. Including the battered remains of the drive.

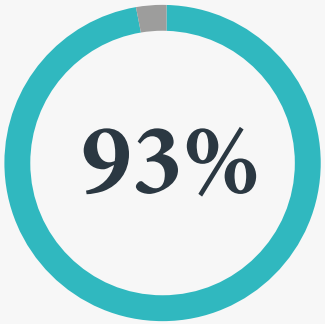
With startling clarity, you suddenly realise this has become a catastrophe of epic proportions.

Here's the reality:

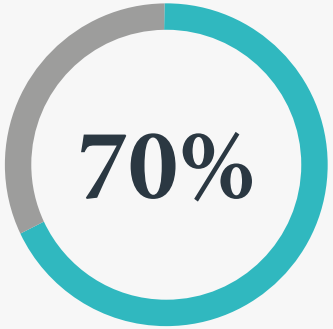
Businesses that lose their data in this way have a greater chance of going under, than surviving

If you think that sentence alone is scary, here are some specific stats:

50% of businesses that lose data due to disaster go into administration



93% of businesses that lose their data for 10 days or more go under within a year



And 70% of businesses that suffer a severe fire go out of business within five years (30% of them do it after just one year)

The stats aren't looking good, are they?

Before you start to hyperventilate, let's go back to the real world. Your office is not on fire and your data – plus your favourite coffee mug – is safe.

Phew.

But with all that in mind, what are the overdue jobs that you keep putting off that – ***if the worst happened*** – you'd be kicking yourself about? What would you wish you'd have done this week?

Here are a few to think about.

A reliable, robust and verified data backup

Let's start with this one since it's the most obvious and easy to get right.

Regardless of the size of your business, having a proper data backup that keeps your data safe all the time, is a basic requirement these days.

And it's not just the prospect of your office burning down that makes your backup a good idea. There are so many other reasons that you might need to access it.

These can be as simple as spilling a cup of coffee over your laptop and accidentally destroying it. Or dropping your laptop. Or leaving it on a train.

Other reasons are scarier. Let's take ransomware as an example. You've heard of this, right?

It's a terrifying type of malware that holds all of your data hostage until you pay a huge ransom to get it back. If you pay the fine, you're still not guaranteed to have your files returned. If you don't pay your files are deleted forever.

The criminals behind ransomware do a lot of advance work to make it very hard for IT partners such as us to stop and fix attacks once they've been launched.

But, although it takes a great deal of work to make your network safe and secured again, you can feel relieved that you might not have lost all your data – if you have a protected backup.

It's really important – and often neglected – to regularly check that the backup is working. The number of times we've had a first time phone call from a panicked business owner, who needed their backup restoring ... only to find that it stopped working months ago. Oops.

There are two aspects to this. There's making sure the backup is happening. And then there's verifying the data to check it is backing up correctly.

What data do you back up? Basically, everything... all data that you've created from all your accounts and projects, right through to your email and website content. If losing any data will have even the slightest impact on your business, back it up.

There are loads of different ways that you can back up your data, and many levels of protection. There's no excuse not to do it. If you're not sure where to start, speak to a great IT service provider who can get the ball rolling.

Protect your devices

Short of locking them in a fire-proof box overnight, you're not going to be able to protect your devices from being damaged in a fire. However, there are certain steps you can take to keep them a little safer.

Our devices can be expensive. Especially when you have lots of them within a business - it soon adds up.

So one of the first things you can do is to make sure they're all insured. Check if they're included in your business insurance, or whether they need to have their own insurance. Make sure you're covered for damage from disaster, but also for theft, and accidental damage too.

Next, make sure that you've thought through what should happen when a device is lost or stolen. Say someone in the business left a laptop in a coffee shop, or they had one stolen from their bag on the train. You now know you're insured, but what about the data on that device? How can you make sure that's protected?

You've hopefully got your data backed up. But you still want to make sure that the information doesn't end up in the wrong hands. Create a procedure called "What should happen if..."

Make sure that everyone in the business knows who to notify should a device be lost or stolen, so that key person can take responsibility for remotely wiping the data.

It's also really, really important to make sure:

1. All data on all devices is encrypted
2. All devices and software are password protected
3. You use multi factor authentication where possible (where you get a code on another device to prove it's really you)

Know what devices you actually have

If your office did burn down, would you honestly know what devices and equipment you've lost?

If the answer to that is no, then I can assure you – you're not alone.

When a business starts to grow, it's easy to lose track of what exactly you've got:

- Who uses which device?
- Who uses more than one?
- What happened to those laptops when they were replaced with higher spec models?

Creating an inventory (and keeping a backed up copy of it) will help you to keep track of everything.

It's also pretty handy to keep an inventory now that so many more of us are working from home. It's easier to lose track when you don't see devices every day! Likewise, if someone leaves the company, you'll know what they need to return to you on their exit.

Go completely paperless

If this isn't something you've already done, start to make the right steps towards it now.

Not only is going paperless better for the environment, but it has so many other benefits for your business too.

Firstly, if your office did have a fire, there wouldn't be shelves, drawers and filing cabinets bursting with additional fuel.

But also, if you did have a fire, there would simply be no way you could get all that data back. And without all of those files in front of you, it could take a long time for you to realise the extent of the information you've lost.

Make your business life a whole lot easier and make a digital copy of everything. Store it securely online, and BACK IT UP!

There are probably many more things you can think of that you'd prefer to get done now, just in case disaster does strike.

Perhaps you could make a list and prioritise them.

When it comes to keeping your business safe, please don't put off the things that you really should do today. Remember those stats we gave you earlier on. The businesses that survive are the ones that are prepared.

If planning for disaster recovery seems like too much work at an already hectic time, give us a call. We'd love to help you get these vital precautions in place, so you can sleep more peacefully at night.

sedcom
Your trusted IT partner

t 0207 998 4151
e craig.butler@sedcom.net
w www.sedcom.net