Cyber-crime: Your business's **5 step plan** to prepare and protect

The world economy loses billions to cyber-crime every year

Cyber-crime: Your business's **5 step plan** to prepare and protect

The world economy loses billions to cyber-crime every year

Billions!

That's a lot of money. And it's a figure that's increased by more than 50% since 2018.

In 2019, two thirds of all organisations reported some type of incident relating to cyber-crime.

You could make a sure bet this figure rose significantly last year, thanks to criminals taking advantage of the pandemic.

It's easy to look at big figures like these, and not relate them back to your own business.

But here's the thing. The average cost of a data breach to a business is estimated to be around £337,000.

The most common types of crime are **ransomware,** where your data is locked away until you pay a ransom fee.

And **phishing,** where criminals pretend to be someone else, to get you to click on a bad link. This is how they get access to critical systems.

That huge average breach figure includes:

- Any ransom demanded by criminals who lock your data and remove your access to it
- The cost of recovering your data, and undoing the extensive damage done
- Putting in place additional ongoing security measures after the breach.

On top of the financial impact, there's the reputational one.

Could you imagine picking up the phone to every single client to tell them your data about them had been accessed and stolen? And was probably for sale on the dark web?

What would happen if the local media or news blogs got hold of this and ran a story about it?

There are other consequences.

92% of businesses that are hacked say there's an enormous impact on company performance.

Plus they lose on average 9 hours of work time, per member of staff.

You have to ask yourself very carefully: Could your business afford to be hit by a ransomware or phishing attack?

Truth is, many small businesses really couldn't.

So why do so few businesses have a plan in place to a) prevent and b) respond to cyber-crime?

It's estimated that more than half of businesses don't have a plan.

Does yours?

If not, it's time to do something about it. There's been an explosion in the number of ransomware and phishing attacks over the past couple of years.

If you're don't have an effective plan in place to keep your business protected – and to minimise damage should the worst happen – you're leaving yourself vulnerable.

Cyber-criminals are targeting all businesses all the time, using clever automated tools that sniff out vulnerabilities. So it's only a matter of time till your business's defences are tested.

Here's our recommended 5 step plan to prepare for an attack, and protect your business.

1 Training, training, training

Believe it or not, your devices and software aren't the weakest link in your defence. **Your people are.**

Your team's awareness of the risks, and their mindset towards spotting risks and acting on them, can make a dramatic difference towards your chances of being affected.

Although they'd never knowingly do a thing to damage your business, all it takes is one click for them to bring you down.

One click. On one bad link. In one email.

Phishing scams are getting more sophisticated every day, and they're really easy to fall for. You don't have to be an 80 year old email newbie to fall for a phishing scam these days. With some of the smartest social engineering, even the wariest person can be caught out.

Fortunately, with the right training, your team can be taught the tell-tale signs of a scam email, looking at:

- The email address it was sent from
- The language used
- The font and design of the email
- How to check if a link is safe before clicking on it

There are other things that cyber security training can teach your people.

Things like closing RDP links; a techy term for a connection from your computer to another.

And looking out for signs you're under attack from ransomware.

Plus other areas of online safety that you may not usually discuss. Such as what information criminals can glean from social media.

There's a lot that can go wrong online. And the more people you have working for you, the greater your risk of one of those things happening to your business.

All staff should have regular cyber-security awareness training – including you.

Things change so frequently that it really is in your best interest to keep everyone's knowledge topped up.

Use the tools available to you

2

There are a lot of tools out there to help keep your business safe and protected from cyber-criminals. **Make use of them.**

Some of the most commonly used tools are:

- **Password managers:** These generate long random character passwords for new applications, and remember them so you don't have to
- **Multi-factor authentication:** This is where you enter a code from another device, to prove it's really you logging in
- **VPNs:** A Virtual Private Network gives you a secure connection to your business when working remotely
- **Encryption:** This makes the content of your devices look like thousands of random characters to anyone without the encryption key. So it's only a minor inconvenience if you lose a device, not a major catastrophe

These are just the basics. There are always extra layers of security available.

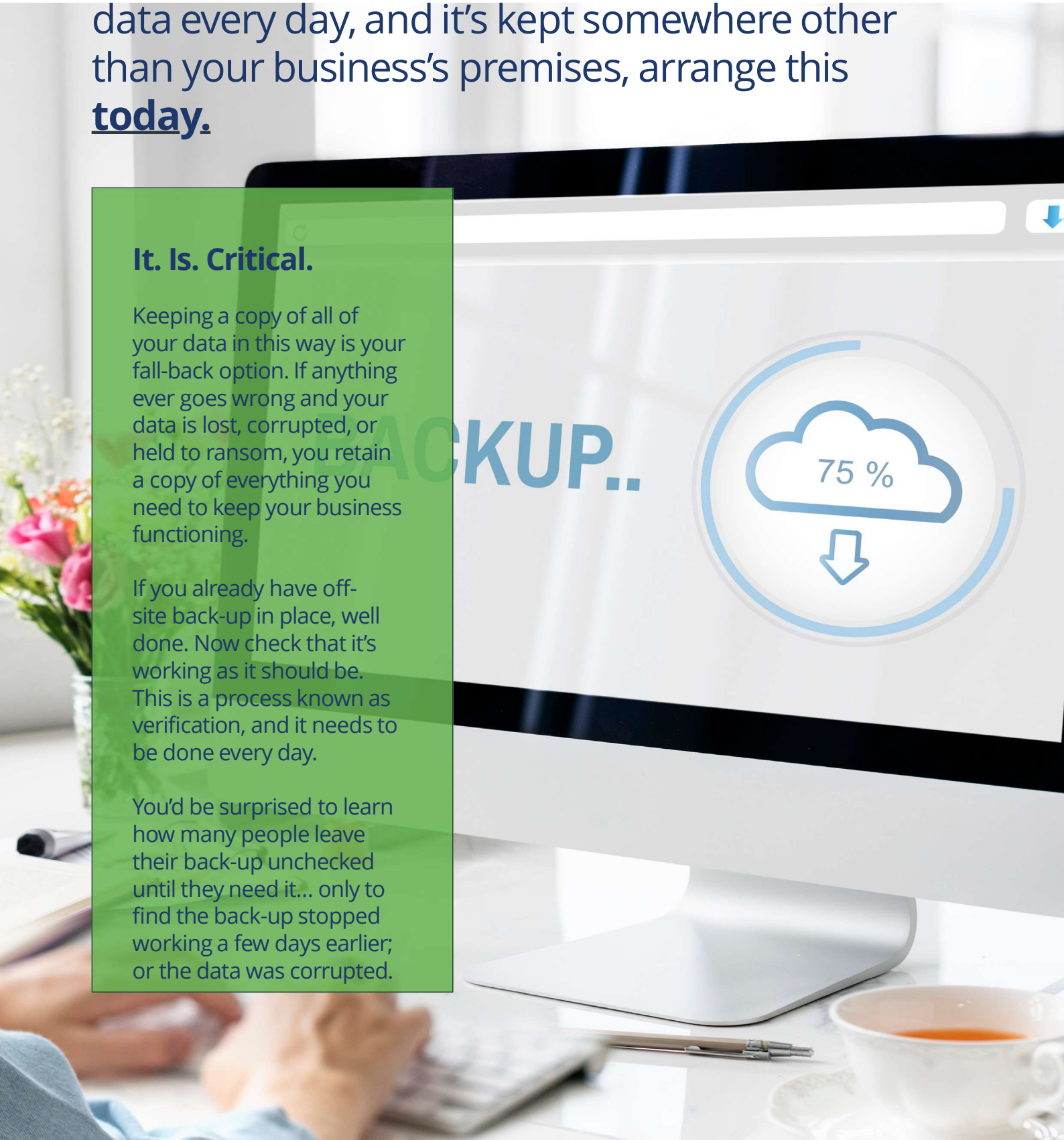
Yes, this is complicated, and there are too many options to choose from. The trick is putting together the right blend of security tools for your specific circumstances.

So you're protected, but your security is not stopping your team from getting on with their work every day.

Your IT support provider will be able to make some recommendations. If you're in the fortune position of having an ***IT partner,*** they will work closely with you to understand how your business works inside and out, before making recommendations.

3 Back-up all data, all the time

We can't stress this enough: if you don't already have an automated back-up of your data every day, and it's kept somewhere other than your business's premises, arrange this **today.**



It. Is. Critical.

Keeping a copy of all of your data in this way is your fall-back option. If anything ever goes wrong and your data is lost, corrupted, or held to ransom, you retain a copy of everything you need to keep your business functioning.

If you already have off-site back-up in place, well done. Now check that it's working as it should be. This is a process known as verification, and it needs to be done every day.

You'd be surprised to learn how many people leave their back-up unchecked until they need it... only to find the back-up stopped working a few days earlier; or the data was corrupted.

PPP

4

Create a policy, protocol, and procedure in the event of a data breach. **Sounds obvious, but this needs to be done before your business has a problem.**

Your policy will set out how your business will deal with any form of data breach or cyber-attack.

Make your **policy** as detailed as possible, as it's a guide for your company to reach the most desired outcome (in this case, minimal impact from an attack).

Include the things your people must do as a minimum to help keep the business safe, such as using a password manager and multi-factor authentication.

Every member of staff in your business should have a copy of this policy, ideally in your company handbook. Maybe you'd even get them to sign that they've read it and are committed to it. That way, no-one can plead ignorance if they've directly put your company at risk.

Your **protocol** is a written plan that contains the procedures your people must follow in the event of a cyber-attack.

And the **procedures** you should include are:

- **Who to alert** in the case of a suspected breach
- **What are the steps** that person should take to try to block the attack
- **How everyone else within the business should react.**

It's a good idea to include a procedure for lost or stolen devices too, so they can be wiped remotely for ultimate peace of mind.

Make everything in your PPP as accurate and detailed as it can be, so that people are left in no doubt exactly what they should do.

If you've never put something like this together before, your IT support provider should be more than happy to help you create your policy, protocol, and procedures.

5 Bring in the experts

If you're not an IT expert, **a lot of this can seem very time consuming and complicated.**

We completely get that.

However, you should understand that it's very much a worthwhile investment of your time and energy.

If you feel it's not something that you can do justice, it's a smart idea to bring in the experts.

A great IT support provider – or IT support partner, in this case – should be more than willing to help you.

In fact, a really great IT support partner will get it all done for you, without you having to prompt them. Honestly; the things we've talked about here are just the basics that you should be doing to cover yourself.

You should also have someone to monitor and maintain your devices and network, to identify and solve the majority of issues before you even notice them.

And someone who can make sure you're using all the right tools and software to optimise both security and staff productivity.

Often, it's unrealistic to have a full-time employee on your team to do this work for you. Fortunately, outsourcing is a superior alternative in most cases.

Not only do you get support when you need it, and benefit from all of the above, but you also get access to a whole array of expertise.

If you don't already have a plan in place to help keep your business protected from cyber-attack, I hope you can see how vital it really is.

If you do have a plan, perhaps it's time to revisit it and make sure it's still effective in this ever-evolving world of cyber-security and cyber-crime.

If you find you could do with some honest, expert help and advice, we'd love to be of service. **Let's talk.**