BE PREPARED:
Sooner or later your business WILL be attacked

5 steps to improve your ransomware resilience

itblue

This is a cold hard fact: Ransomware is on the rise

Here's a quick Q&A answering the most common questions about it.

What is it?

It's where hackers break into your network, encrypt your data so you can't access it, and then charge you a large ransom fee to unlock it. It's the most disruptive and costly kind of attack you can imagine. And very hard to undo.

Why is it a big deal?

Ransomware attacks are dramatically up thanks to the pandemic. All the urgent changes that businesses went through last year created a perfect storm, with plenty of new opportunities for cyber criminals.

Is my business really at risk?

Thanks to automated tools used by hackers, all businesses are being Targeted, all the time. In fact, hackers prefer to target small businesses as they typically invest less time and money into preventative security measures compared to large companies.

It's estimated a business is infected with ransomware every 14 seconds. And the hackers can demand thousands and thousands of pounds to unlock your data... with no guarantee they will actually comply once you've paid.

How can my business get infected with ransomware?

42% of ransomware comes from phishing emails, this is where you get a legitimate-looking email asking you to take a specific action. You only need to click a bad link once to let attackers quietly into your system. And it doesn't have to be you who clicks... it could be any member of your team.

Malicious websites make up 23% of attacks. And compromised passwords account for 21% of ransomware attacks.

Why is it so hard to undo?

A ransomware attack takes weeks for the hackers to set up. Once inside a network, they stay hidden and take their time to make lots of changes. Essentially, they're making it virtually impossible for an IT security company such as ours to undo the damage and kick them out once the attack has started.

If you haven't thoroughly prepared for a ransomware attack before it happens, you are much more likely to have to pay the fee.

How much is the typical ransom?

The hackers aren't stupid. They know trying to get R1 000,000 out of a small business simply won't happen. But you might stump up R50,000 just to end the hell of a ransomware attack. They will change their ransom demand based on how much money they believe a business has.

Nearly 50% of businesses are so under prepared they have to pay the ransom to get their data back.

Of course, the ransom isn't the only cost associated with an attack. There are countless indirect costs. Such as being unable to access your data or systems for a week or longer. How horrendous would it be if no-one could do any work on their computer for a week? How would your customers react to that?

Post-attack, productivity is always damaged, as staff get used to new systems, ways of working and greater security measures.

What can I do now to protect my business?

This is the most important question to ask. It's virtually impossible to stop a ransomware attack from happening. But you can do an enormous amount of preparation, so if an attack does happen, it's an inconvenience, not a catastrophe.

Here are the 5 steps we recommend for maximising your ransomware resilience.

Act as if there's no software protecting you

#1

Software is essential to keep your business safe from all the cyber security threats. But there's a downside of using this software – it can make you and your team complacent.

Actually, humans are the first defense against cyber-attacks. For example, if your team doesn't click on a bad link in a phishing email in the first place, then you're not relying on software to detect an attack and try to stop it.

This means basic training for everyone in the business, and then keeping them up-to-date with the latest threats. This has got to be done in a way that's fun! No-one wants to do boring techy training... (not even us, and this is our passion).

Make sure your IT partner has robust systems in place

#2

You must have robust data protection and system security in place, including software that only allows approved apps to be used on your network.

From your IT partner, you need an appropriate blend of reactive and proactive support.

Reactive support is critical in situations where a ransomware attack is successful. It means you have experts on hand immediately, to minimise the impact and get your business up and running again as quickly as they can.

But, long-term, proper proactive support is vital. This means you have someone working away in the background, keeping your systems safe and 100% updated. They're looking out for problems on the horizon, and spotting anything out of the ordinary. This also means you'll have less disruption from issues, as the majority can be resolved before they impact you or your team.

In the case of a suspected ransomware attack, a proactive IT partner will already have a protection and recovery strategy that they can trigger immediately.

Invest in the best data backup and recovery you can

#3

Automatic off-site data backup is a business basic. When you have a working backup in place, it can be tempting not to give it a second thought.

But, it's worth remembering that cyber criminals will take any means necessary to get you to pay their ransom. That means they'll target your back-up files too, including cloud-based data.

It's critical that you create and implement a comprehensive back-up and recovery approach to all of your business data.

The National Cyber Security Centre sets out a cyber security framework which includes best practices such as:

- **Constant backups:** Separate from the computers and ideally in the cloud
- **Immutable storage:** This means once created, backups can't be changed
- **Firewalls:** To restrict what data gets in and out

#4

Create a plan for cyber-attacks

When a cyber-attack happens, every second is crucial. The earlier you take action, the less damage is caused.

So prepare a detailed plan of action and make sure everyone knows what's in it, where to find it, and how to trigger it.

Test your plan regularly to make sure of its effectiveness, and remove any risk of failure by keeping at least three copies of it in different places. One should be a printout kept at someone's home... just in case you have zero access to data storage.

Work out what data and systems are vital to the running of the business, and what you can do without for a short time. When an attack happens, you then know what apps, software and data should be prioritised for recovery.

#5

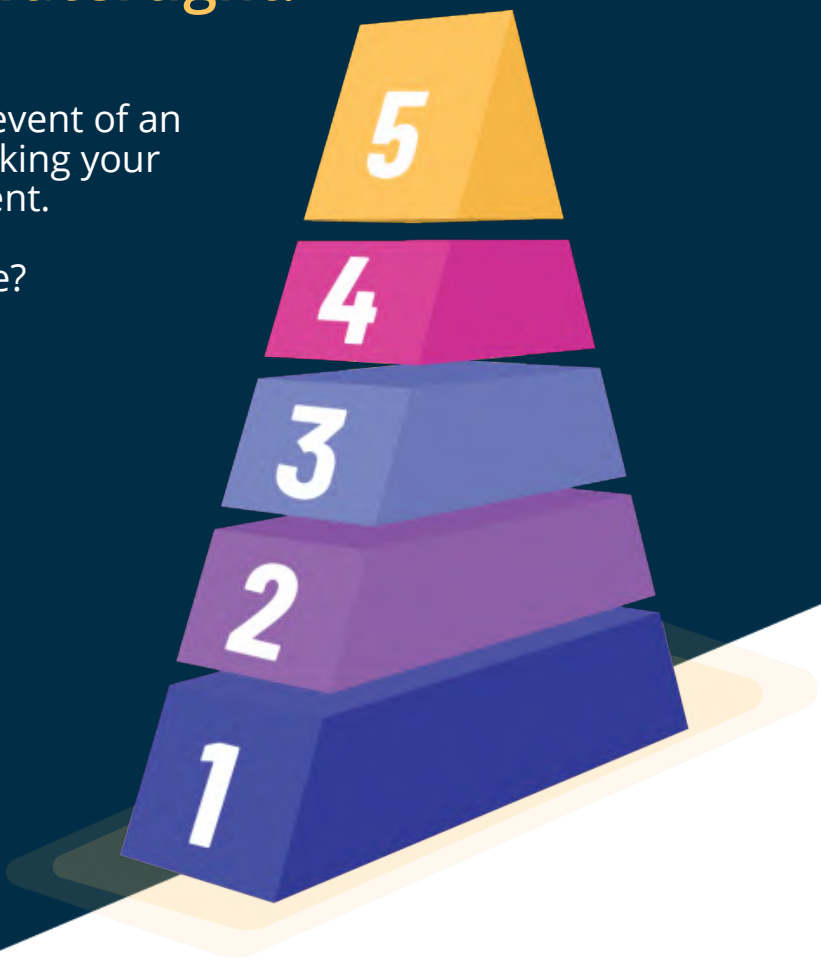
Prepare, prepare...and prepare some more

By creating a layered approach to recovery, you're effectively reducing the impact of any ransomware attack. The sooner you can get your business back up and running, the less money you'll lose and damage you'll suffer. And your customers are less likely to lose faith in you.

The big take away from this guide is that it's 100% impossible to protect your business from cyber-attacks. While your trusted IT support partner can create a highly secure system around you, realistically, it will never be 100% watertight.

By planning for what happens in the event of an attack or attempted attack, you're making your business far more ransomware resilient.

There's a lot to take in here, isn't there? For our clients, we do as much of the hard work for them as we can.



Are you ready to choose a new IT partner? Let's talk.

Reach out to us today for a no obligation conversation :

- **21 880 2796**
- **info@itblue.co.za**

itblue