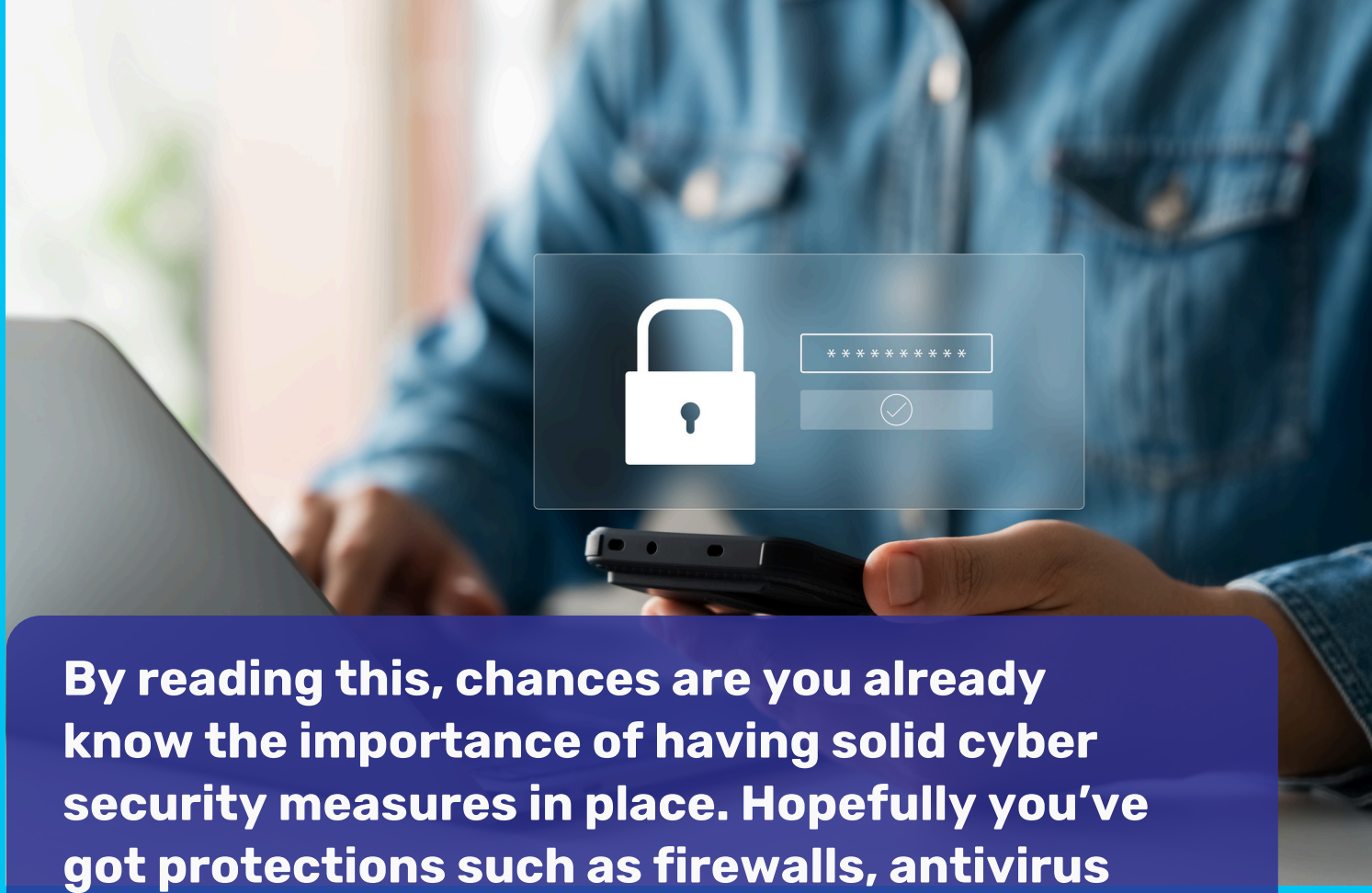
Cyber Security

# **5 steps** to help recover from a cyber attack

IT CONSULTANCY I SERVICES I SOLUTIONS

www.uk-it.uk




**By reading this, chances are you already know the importance of having solid cyber security measures in place. Hopefully you've got protections such as firewalls, antivirus software, and multi-factor authentication (where you get a login code from another device). Great work!**

But here's the thing: No matter how many security measures you have in place, there's always a chance – however small – that someone might breach your defences. No system is 100% foolproof. It's like having the most advanced lock on your front door… sure, it'll keep most burglars out, but if someone really wants to get in, they'll find a way.

Cue the dramatic music.

You see, while having all those security measures in place is crucial, it's equally important to have a plan for when – and not if – the worst-case scenario happens. Prepare for the worst while hoping for the best.

So, how do you plan for a cyber attack if you don't know what you're expecting, or when you're expecting it?

Good news: It's easier than you might think. To help you get started with your own recovery plan, we've broken things down into 5 steps. Follow these and you can rest assured that even if the worst happens, you and your team will know the best way to react to save your business from damage and disruption… and you from the mother of all headaches.

# Step 1: Assess the damage

**When your business is hit by a cyber attack, it can feel like a punch in the gut and leaves you scrambling to figure out what to do next. Instead of taking wild guesses or hitting the panic button, take a methodical approach to work out what exactly you're dealing with.**

First things first, take a moment to breathe. It's easier said than done when your heart is racing and your mind is swirling with worst-case scenarios, but a clear head is your best ally in this situation.

Round up your team, gather everyone in a room (virtual or physical), and let them know what's going on. It's important to have all hands on deck to tackle the challenge together.

Now take stock of the damage. What systems or data have been compromised? Are there any immediate threats you need to address? Take notes, gather evidence, and try to get a clear picture of the situation.

Next, try to figure out how the attackers got in. Was it through a phishing email? A vulnerability in your software? Understanding what's known as the 'attack vector' will help plug the hole and prevent future breaches.

# Step 2: Contain the breach

**Once you have a handle on the situation, it's time to contain the breach. This might involve shutting down compromised systems, isolating infected devices, or blocking suspicious network traffic, as well as changing your passwords. The goal is to prevent the attack from spreading further.**

Depending on the severity of the attack and the nature of your business, you may need to notify the relevant authorities. This could include law enforcement, regulatory agencies, or industry watchdogs. Don't be afraid to ask for help if you need it.

# Step 3: Restore your systems and data

**OK, crisis averted. Now there are some steps you need to take to begin the restoration process and get back to business as quickly as possible.**

## Prioritise critical systems

Not all systems are created equal. Start by identifying the systems and data that are essential for your business operations. These might include customer databases, financial records, or production systems. Focus your efforts on restoring these first.

## Restore from backup

Lost all your data? Don't panic, that's why you've got backups. Restore your systems and data from the most recent backup available. Make sure to verify the integrity of these first though. Some attacks can compromise them too.

## Patch and update

Once your systems are back online, it's important to patch any vulnerabilities that may have been exploited during the attack. Update your software, firmware, and security patches to make sure you're running the latest, most secure versions.

## Test, test, test

Before declaring victory and going back to business as usual, you need to test your restored systems thoroughly. Make sure everything is functioning as it should be and there are no lingering issues or vulnerabilities.

## Communicate with stakeholders

Keep your stakeholders informed throughout the restoration process. Let them know what happened, what you're doing to fix it, and when they can expect things to be back to normal. Transparency will help you maintain their trust and confidence.

## Step 4: Learn and adapt

**Congratulations, you've survived a cyber attack. But before you kick back and relax, there's one more thing you need to do: Learn and adapt for next time. Because let's face it, there's usually a next time. What lessons have you learned from this experience? What changes can you make to your security posture to better protect your business?**

### Conduct a security audit

Start by taking a close look at your existing security measures. Are there any gaps or weaknesses that need to be addressed? Conduct a thorough security audit to identify vulnerabilities in your systems, processes, and policies.

### Implement multi-layered security

One of the most effective ways to defend against cyber threats is to implement a multi-layered security approach. This means using a combination of technologies and techniques, such as firewalls, antivirus software, intrusion detection systems, and employee training, to create multiple barriers against attacks.

### Encrypt sensitive data

Encrypting sensitive data adds yet another layer of protection, making it much harder for attackers to access and exploit. Make sure to encrypt data both in transit (that's when it's being sent from person to person/place to place) and at rest (when it's saved in your systems). For maximum security consider implementing end-to-end encryption, where only the sender and recipient can decode the data.

### Enforce strong password policies

Weak passwords are a cyber criminal's best friend. Enforce strong password policies across your business, requiring employees to use long randomly generated unique passwords. A password manager can make this simpler and safer. Strongly consider implementing multi-factor authentication for another layer of security.

### Stay up to date with security patches

Cyber threats are constantly evolving, so it's crucial to stay on top of security patches and updates for your software, firmware, and operating systems. Make sure to apply patches as soon as possible to stop attackers exploiting known vulnerabilities.

### Educate and train employees

Your employees are your first line of defence against cyber attacks. Educate them about the importance of cyber security and provide regular training to help them recognise and respond to potential threats. Teach them how to spot phishing emails, avoid suspicious websites, and practice good security hygiene.

### Monitor and respond to threats

Real-time monitoring and alerting systems will help you detect and respond to potential security threats as soon as they arise. Set up regular security audits and penetration tests for a proactive approach.

## Step 5: Develop an incident response plan (BEFORE you need it)

**No matter how strong your defences, there's always a chance that you'll be targeted by cyber criminals again. That's why it's vital to have a solid incident response plan in place to help you respond quickly and effectively in the event of a cyber attack.**

**In fact, don't wait to be targeted the first time. Create your incident response plan now, before you need it, and stay one step ahead.**

### Create your incident response team

The first step in developing an incident response plan is to set up a dedicated team who will be responsible for handling cyber security incidents. This team should include representatives from IT, security, legal, communications, and other relevant departments. Make sure everyone knows their roles and responsibilities in the event of an incident.

## Identify and prioritise threats

Next, identify the types of cyber threats that your business is most likely to face and prioritise them based on their potential impact. This will help you focus your resources on mitigating the most significant risks and developing targeted response strategies.

## Develop response procedures

Once you've identified the threats, develop detailed response procedures for each type of incident. This should include step-by-step instructions for detecting, containing, and mitigating the impact of the incident, as well as communication protocols for notifying stakeholders and coordinating the response efforts.

## Test and refine your plan

A plan is only as good as its execution, so test your incident response plan regularly through tabletop exercises and simulations. This will help identify any weaknesses or gaps so that you can refine it accordingly. Make sure to involve all members of your incident response team in these exercises to ensure everyone knows what to do in the event of an incident.

## Communicate effectively

Communication is key, so make sure everyone involved in handling an incident knows their role, but also tell everyone in the business about the incident response plan. Anyone could be the first to sound the alarm, so everyone needs to know who to report any incidents to in the first instance.

**If you need help or advice, we'd love to talk about how we can help your business. Get in touch.**

**CALL: 0330 223 0005**
**EMAIL: hello@uk-it.uk**
**WEBSITE: www.uk-it.uk**

IT CONSULTANCY I SERVICES I SOLUTIONS