

Ransomware disaster response plan template



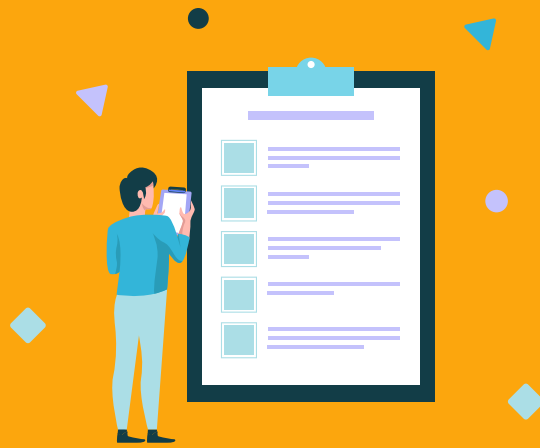


Table of contents

Introduction	3
First thing's first: what is a disaster recovery plan?	5
Preventative measures	6
Your creative agency's ransomware disaster plan	9
Outsmart an evolving threat	13

Definition: Ransomware (Noun)

A type of malicious software designed to block access to a computer system until a sum of money is paid.



Ah. Ransomware. It's a nasty sounding malware – one that's very deserving of its name.

In May 2017, a ransomware attack brought the NHS to its knees. Considered to be the [largest](#), most aggressive ransomware case of its kind, the global attack infected over 300,000 computers in 150 countries. The criminals were demanding up to \$300 per computer in ransom, and the attack resulted in hospitals having to turn away patients.

Now, as a creative business, you may question the relevance of a healthcare case study. But, ransomware isn't isolated to a particular industry or company; successful ransomware attacks hit [33 percent](#) of all organisations.

And, unfortunately, these attacks are only growing. In fact, since the beginning of 2019, they've grown by [118 percent](#). To combat this increase, your business should hope for the best, but plan for the worst.


In this short guide, we'll discuss the importance of having a disaster recovery plan in place and why you should embrace the best preventative techniques. We'll also provide you with a step-by-step ransomware response plan, should an attack ever occur.



First thing's first: what is a disaster recovery plan?

A disaster recovery plan (DRP) is a step-by-step guide to minimising the damage a data breach or malware can cause. It involves aligning your recovery action with your key business priorities, helping you to navigate the 'aftermath' of any ransomware attack.

As J.R.R. Tolkien once said:



'It does not do to leave a live dragon out of your calculations, if you live near him.'

While your DRP may not be as glamorous as donning your armour and riding into battle, it's still necessary to protect your business with a watertight battle plan.

Before you create a detailed plan, be sure to perform a [business impact analysis](#) to establish the key areas you need to protect and recover.

For a creative business – such as a marketing agency – this might be your client's contact data. As a result, your DRP should involve data backup and restoration initiatives.

But, let's take a step back a moment. Protecting yourself from ransomware works best when you don't wander into a dragon's lair in the first place. That's why you must take preventative measures.

Preventative measures

When it comes to protecting yourself against ransomware, prevention is better than a cure. While every business should have a solid DRP in place, there are plenty of ways to reduce the possibility of an attack before it happens.

Here are five areas for your agency to consider:

1. Anti-malware software

At its heart, anti-malware prevents, detects and removes malicious software in your IT systems. With [90 percent](#) of UK businesses using anti-malware software, it's clear that it should act as an essential element of your disaster prevention plan.

However, while anti-malware is an effective way to protect your business against ransomware, due to the growing sophistication of cyber attacks it is no longer a 'fix all' solution. In fact, experts now advise a protection strategy that is both [multi-layered](#) and tailored to your business needs.

2. Training employees in cyber security

While you could invest every penny in the latest technology on offer, if you lack proper cyber security training, your business will always be vulnerable to ransomware.

As it stands, only [one in five](#) businesses invest in cyber security training. This, of course, means that four in every five companies are left vulnerable to ransomware attacks – many of which are caused (albeit accidentally) by [your own employees](#).

Though you might not consider yourselves techies, frequent, up-to-date training is essential for keeping your agency safe. More than that, it can also create an atmosphere where employees can speak up and report suspicious activity.

Better still, modest investments in cyber security awareness and training has a [72 percent](#) chance of significantly reducing the business impact of a cyber attack. That's pretty preventative, if you ask us.

3. Use firewalls

With [43 percent](#) of UK businesses using them, firewalls are one of the oldest forms of IT security around. They work by creating a filter between your private files and the internet, helping to keep your sensitive data out of the wrong hands.

4. Back-up your data regularly

One of the ways ransomware differs from other cyber attacks, is that the criminals hold your data hostage in order to secure a ransom (often in the form of cryptocurrencies). Unfortunately, even after paying this ransom, your agency isn't guaranteed to get your data or creative work back.

So, the best way to ensure you do not lose previous data is to run regular backups. By performing frequenting data backups, you keep the upper hand. After all, they can't extort you if you haven't lost anything.

5. Ensure you use strong passwords

LinkedIn once suffered a [catastrophic data breach](#). The cause? Pathetic passwords. In fact, almost 800,000 members of the social media platform were using the password, '123456'. (Yes, really.)

If your team is predominantly non-techy, the chances are their passwords might not be the strongest.

But, unfortunately, [hacked passwords](#) cause 81 percent of all data breaches and can be the gateway for ransomware attacks. In order to keep your creative work, employees and clients safe, consider using a [password manager](#) or invest in software that boasts multi-factor authentication.

Your creative agency's ransomware disaster plan

With ransomware attacks becoming more and more sophisticated, even the strongest prevention plan could fall through.

But, don't panic. We've created a clear-cut ransomware disaster plan for your creative business.

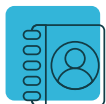
Phase 1: Discovery

So, your agency's data is being held ransom. What should you do post-discovery?



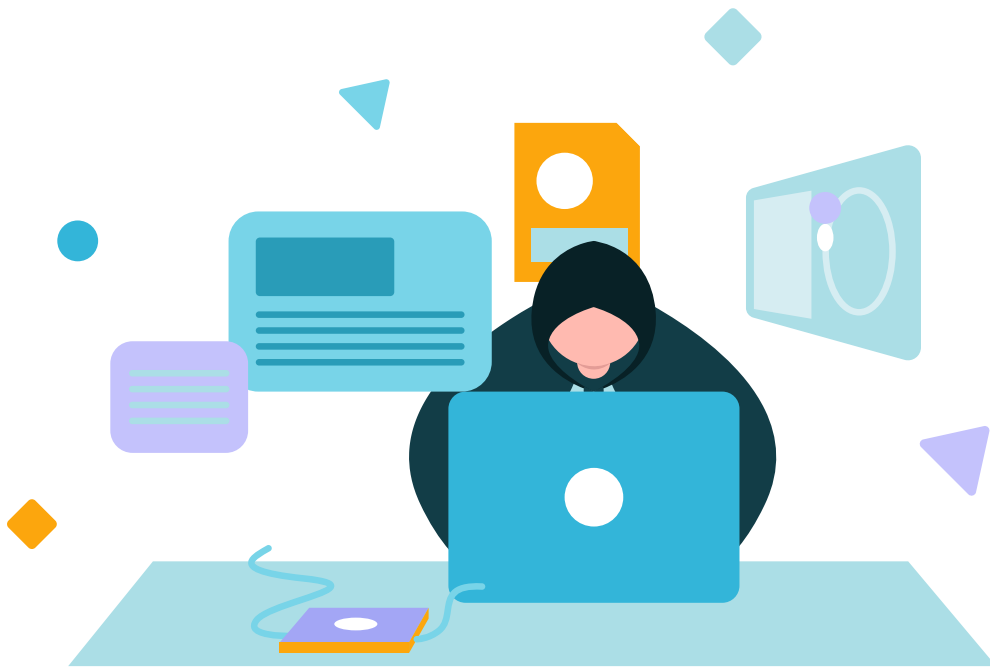
1. Do not pay the ransom

Put your wallet back in your pocket. Attackers will try to take your data hostage in exchange for money, but don't take the bait. Remember, you're dealing with criminals; don't negotiate with terrorists.



2. Contact your IT team or external IT partner

Any IT partner worth their salt will have an effective strategy for dealing with ransomware. They should be your first port of call when you're under attack, so once you've discover the malware, contact them immediately.



Working with a trusted partner greatly decreases the steps your agency will have to take to prevent an IT disaster. Indeed, outsourcing your cyber defence to a team of experts can be the difference between an attack being a mere inconvenience or a devastating blow to your business.



3. Report a breach

If the ransomware has taken sensitive data, such as your client's personal information or their customers' details, you must first assess the damage and severity of the incident. If you feel as though it poses a risk, you must [report the breach to the ICO](#).

Under the [GDPR](#), this is crucial for ensuring the right legal steps are taken to help protect your data subjects.

Phase 2: Isolation

Next, you'll want to isolate the malware.



1. Disconnect all infected hardware

Prevent the attack from spreading by disconnecting all infected hardware. This will help to minimise the damage and prevent the hackers from taking any more of your data hostage.



2. Run security scans

Using your anti-malware software, run a security scan to find the source of the ransomware.

Phase 3: Destruction and documentation

You've found the bug in your system – now it's time to send in the extermination team.



1. Delete the malware

Once located, delete the virus. (Good riddance!)



2. Document the attack

Throughout the attack, someone in your company (or your IT partner) should document every occurrence. Once everything is under control, you can share these notes with the appropriate authorities and the police.

All being well, this should hopefully lead to the attackers facing justice and your business keeping its reputation intact. You can demonstrate how you fixed the incident and how you plan to prevent something similar happening again. This means that both your clients and employees maintain complete confidence in the security of your agency.

Phase 4: Recovery

Next, focus on getting your business back on its feet.



1. Reinstate data

Hopefully, you will have backed up your data safely out of reach from the ransomware criminals' grasp. If so, reinstate your last backup onto clean machines. Your business should be back in working order.



Outsmart an evolving threat

Ransomware is yet another threat that your business must anticipate. As a digitally focused creative business, your employees likely work from computers or portable devices throughout the working week.

And that makes you a target.

With new strains of ransomware appearing frequently, it's doubtful experts will ever find a complete solution to deter cyber criminals. That's why you shouldn't stop at purchasing anti-malware. In order to keep your crucial data safe, you must create a strong, multi-layered prevention and disaster plan.

While all this may sound a little scary, particularly to those of you who don't have a dedicated or substantial IT, keep a cool head.

If you lack the in-house expertise at your agency, find a trusted IT partner who will ensure your data is kept out of the wrong hands.

So, are you in the market for peace of mind? Check out what Pensar [could do for you](#).