epoq IT

www.epoq-it.co.uk

Your disaster recovery checklist

IT security is something that many SMEs pay little attention to. Surely the risk is low when you've only got a handful of computers? And cybercriminals are more interested in large companies?

Actually, the threat to growing businesses is significant – 63% of SMEs have experienced a data breach – and you don't have the same global reputation as major enterprises, or financial resources to deal with the impact.

The best way to combat business IT threats is to plan ahead, by putting a disaster recovery plan in place. To help you reduce risks, ask yourself these questions and complete our quick checklist:

☑ Have you conducted a business impact analysis?

A good disaster recovery plan covers every eventuality, but the reality is that some crises will be more costly than others. Which security problems would cause the most damage to your reputation? What threats could you manage internally, and which events would require specialist help? How long can you shut down operations without it putting your finances at risk?

Before you start to plan for the worst, write a business impact analysis looking at the consequences of common security breaches. This will help you assess the various threat levels of mistakes and cyberattacks, and get you thinking about the process you'll need to contain incidents quickly and effectively.

☑ Have you set recovery time and point objectives?

With a business impact analysis in place, the next step is to use this insight to set a recovery time objective (RTO) and recovery point objective (RPO) for security breaches. An RTO is the amount of time you need to fix a security issue in order to move forward without it impacting business operations. Once you pass this point, customers will start to feel the impact of your problems.

An RPO is similar to an RTO, except it measures the amount of time before a significant or unsustainable level of data is lost from your business. This will be determined by how frequently you back up data. It may even prompt you to put a better backup system in place!

With an RTO and RPO, you have a good idea of how long your company has to deal with a security problem before it has deeper, longer-term consequences.

☑ Do you have a complete inventory of office equipment?

When you're busy getting work done, it's easy to order new technology without keeping a complete record of everything you own. But when a security breach takes place, having an up-to-date inventory can help you resolve problems quicker.

In addition to the computers, smartphones and other technical devices you're using, it's worth recording all the security software you've licensed. List details of when those licenses expire, so you aren't left in a situation where they've stopped working and nobody has renewed the subscription.

☑ Who is on your disaster recovery team – and what are they looking after?

One of the major reasons that businesses of every size need a disaster recovery checklist is to make sure that everyone plays their part in protecting your company.

It's really easy for people to assume that data, software and technology security is someone else's responsibility. This can lead to staff ignoring potential problems, assuming a colleague will sort it out, or even directly contributing towards poor security practices.

The best way to make business protection a team effort is to give everyone a role, and document responsibilities clearly. Go back to your business impact analysis and list every type of security threat: this is the basis of your disaster recovery plan. Assign the response for each threat to someone in your business, so you know there's protocol in place.

It's important you take a formal approach to disaster recovery, so your team consider their duties seriously. Everyone should have a written record of the actions they are expected to safeguard, plus details of what they should do in the event of a security issue.

☑ How will you update staff, suppliers and customers?

Assigning roles and responsibilities to team members will help you to identify and report potential security issues quickly. However, it's important that you also put communication chains in place as part of your disaster recovery plan, to keep key stakeholders up-to-date.

The first chain of command you need to establish is internal. If you grew up in the pre-mobile era, you'll remember schools issuing a 'telephone tree'. One parent would pass on an important message to the next; for example, when the bus was due to arrive back from a school trip. Building a similar contact chain for your staff – which includes their telephone details, in case email programmes have been struck down – will speed up response times and share the burden of disaster response.

The next chain of command you need to consider is external. Often a security breach can affect your suppliers or customers. For example, a cyberattack takes your website down or blocks email communications.

Make sure you have an up-to-date supplier and customer database, which is stored securely somewhere that can be accessed even if your main network goes down.

Your disaster recovery plan should outline in which scenarios external stakeholders, and the best way in which to contact them. If you have marketing or PR resources, it's a good idea to involve them here, so they can help to limit damage from a reputation perspective.

☑ Do you have the expertise to deal with security breaches in-house?

It doesn't matter what targets you set or how tight your chain of command is – if you can't fix the problem, a security breach will prove costly!

While large enterprises have the budget to employ large in-house teams to monitor threats, mitigate issues and launch responses, SMEs can't afford the same level of resource. Which is why many start-up and scale-up businesses outsource IT security to a managed services provider.

An external IT partner will take the burden of business security off your shoulders, providing round-the-clock monitoring to identify, manage an, where necessary, alert you to potential threats. Your partner should put measures in place to reduce your security risk – from GDPR-compliant data storage, to installing the latest antivirus and malware software on all your technology.

Depending on the support package you choose, managed service providers can even deliver a tailor-made disaster recovery plan on your behalf, which factors-in potential threats and outlines expert-driven responses for each scenario. And the monthly subscription is so much more affordable than hiring a full-time in-house IT expert.

☑ When was the last time you reviewed your disaster recovery plan?

All of the disaster recovery points we've discussed should not be considered a one-time requirement. As your business grows and threats evolve, the risks and vulnerabilities you face will change.

Regularly reviewing your disaster recovery plan is essential to optimising business security. If you're hit by a cyberattack, a year-old plan will prove useless if the person in charge responding has left the company, it's affecting a new piece of software that nobody is responsible for, or you don't know how many computers your business owns to check which devices have been affected.

And in the unfortunate event that you are hit by a cyberattack, it's important that you learn from this event and put measures into your disaster recovery plan to limit future damage.

One of the reasons that SMEs choose to outsource business IT is to ensure disaster recovery plans are being regularly reviewed and updated disaster. As industry experts, it's your managed service provider's job to learn about emerging cyberthreats, adapting the plan as your business grows and scales.

Disaster recovery checklist

- ☑ Conduct a business impact analysis
- ☑ Set recovery time and recovery point objectives
- ☑ Create an inventory of office equipment and software subscriptions
- ☑ Frequently backup data
- ☑ Establish a disaster recovery team and give everyone clear responsibilities
- ☑ Maintain up-to-date supplier and customer lists and store them securely
- ☑ Build a contact chain to roll-out in the event of a disaster
- ☑ Review your disaster recovery plan regularly and update it if necessary
- ☑ Outsource your business IT if you have any concerns about handling a security issue

Epoq-IT specialises in managed IT services for SMEs. Our 'My Recovery' package covers the wide-ranging complexities of IT risk management, delivering tailor-made disaster recovery plans for your business for an affordable monthly subscription.

→ Learn more about Epoq-IT's disaster recovery planning service

→ Download the SME e-book for more information about our comprehensive value solutions for managed services

About Epoq IT

Epoq IT builds long-term relationships with businesses that simply want their IT systems and technology to support their stability, growth and competitive edge.

We also specialise in helping organisations operating in regulated sectors to achieve and demonstrate compliance with services that span IT Strategy, IT Security, Business Continuity, Digital Transformation and fully Managed IT Support.

A complete solution for managing your IT strategy and effectiveness, our award-winning IT Managed Services, and Consultancy Services are flexibly designed to meet your business needs.

Email us
Call: 01494 976939

Follow us on: