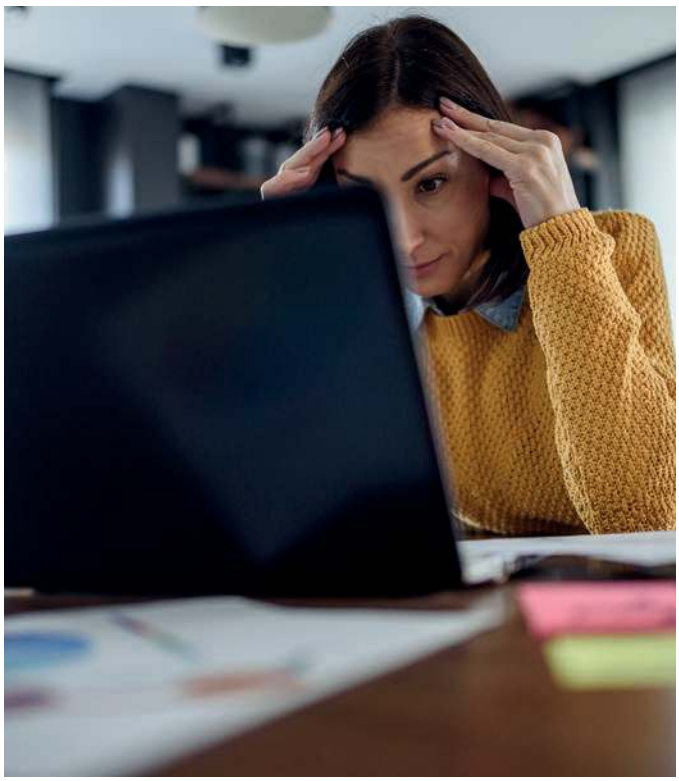
RISK SOLUTIONS

Why you should consider cyber insurance?



1) Remote working

Since the pandemic started, working from home has become widespread across the normal working culture in the UK. While working from home is convenient and has many benefits, it also exposes both individuals and businesses to a range of cybersecurity risks.

When employees work remotely, they're often using their personal devices to access the business network, even the smallest businesses will operate on a cloud based network.

Organisations often overlook the security situation of their employees' home WiFi network or even a public WiFi such as shared-working space, coffee shop or eatery. When people think of security hygiene and their personal devices, it's easy to lose consciousness of the networks they use for remote working. WiFi Routers need to be updated and maintained just like any other piece of hardware, yet most people forget about it completely - employees are actively leaving businesses exposed without even being aware.

Most malware and ransomware is delivered via phishing email attacks, and target people working from home or public access points.

2) Your data is outsourced It's still a data breach risk!

Imagine what happens in the event of a data breach. If an organisation outsources their data to a third party and that third party is breached, they could be forgiven for thinking that responsibility for notifying affected individuals and dealing with any subsequent regulatory actions that may arise would rest with the breached third party.

If personal data is entrusted to an organisation, they are responsible for looking after that data, regardless of whether or not a third party is utilised to process or store it. If that data is lost or stolen, then it is the organisation that will be accountable for any notification requirements, regulatory investigations, fines, or penalties that do arise, and it will be their reputation that suffers, not the third party's.

2.1) We don't collect sensitive data

Cyber insurance is about much more than a data breach and privacy risk. In fact, two of the most common sources of cyber claims are funds transfer fraud or business interruption as a result of ransomware.

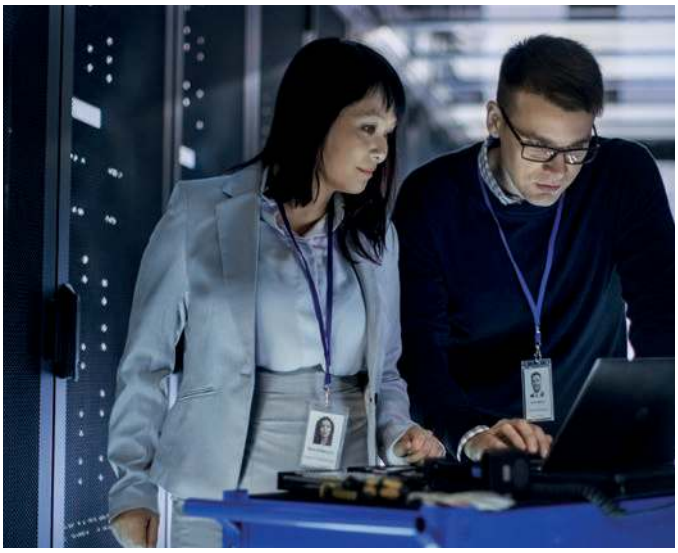
Any business that transfers money to and from a business bank account is susceptible to funds transfer fraud, and many of the victims of these losses hold next to no sensitive personal data.

Ransomware outbreaks cripple many organisations with recent large-scale attacks not involving the theft of data, but rather the freezing or damage of business-critical computer systems.

3) Complete reliance in 3rd party IT providers

The most common objection to purchasing a cyber insurance policy. Not purchasing a cyber policy because you have "Good IT security" is similar to suggesting that an organisation doesn't need theft cover on a property policy because you have high quality locks on your doors, or fire cover because you have a new sprinkler system in place. There is a big difference between vulnerability and risk.

No matter how much a company invests in IT security, they will never be 100% secure. The purpose of an insurance policy is to respond in the event that the worst happens, with experts on hand to manage the situation and financial remuneration for the costs involved.



4) Small businesses are seen as an easy target for cyber criminals

With the headlines focusing on major security breaches at enterprise companies, small and medium sized businesses are far more common victims of cyber attacks. In fact, it is estimated that small businesses are being hit with upwards of 10,000 attacks daily. Even though the rewards may be less financially, cybercriminals see smaller organisations as low-hanging fruit due to lack of resources. SMEs usually invest less in IT security with mostly outsourced operations and third party vendors. This also results in less training for their staff on cybersecurity risks due to the busy daily demands of an SME business.

Key Cyber Risk Statistics

From UK Gov Cyber Security Breaches Survey 2021

39% 39% of businesses report having cyber security breaches or attacks in the last 12 months

£ Average cost of all the cyber security breaches in the past 12 months is estimated to be £8,460

50% 50% of businesses say they experienced at least one cyber security incident – excluding phishing – in the last twelve months

77% 77% of businesses say cyber security is a high priority for their directors or senior managers

What you can do to reduce the price of your cyber premium?

Insurers want to see businesses taking a proactive approach to managing their cyber risk. This is always a difficult task for many SMEs in the UK. By implementing the best security practices, you will reduce your premiums, while most importantly, improving your organisation's cybersecurity. After all, the real goal is to prevent and significantly reduce the likelihood of a cyberattack or loss of data.

1

Have an Incident response plan!

Make sure your organisation has an updated cyber incident response plan. The plan should be comprehensive, identify key team members and decision makers, and include communications strategies, notification requirements, and incident response vendor contacts. Most importantly, the plan should be practiced, regularly reviewed, and updated.

2

Backups taken regularly

Whether your data is on site or in the cloud, protect it with a backup and recovery solutions to ensure timely restoration that meets or exceeds the expectations of your incident response plan.

3

MFA enabled

Use multi-factor authentication before providing anyone access to networks, servers, applications, systems, or data, and always use multi-factor authentication for remote access. These two processes make it much harder for unauthorized persons to steal sensitive data or access your business network. It's just like locking the door and then a further deadbolt to prevent a break-in.

4

Cyber Training

Cybersecurity awareness training is a must for any business in today's world. Your employees can be the weak link in an otherwise strong chain of IT security. Security training helps people understand their role and limits the risk that an employee falls for simple scams such as phishing or social engineering tactics used by cyber criminals.

5

Close and protect ports

Remote Desktop Protocol (RDP) allows users to access their office desktop and computing resources remotely. While convenient to businesses and individuals, it can also make businesses extremely vulnerable to ransomware attacks if not secured correctly. Its estimated that over half of the ransomware attacks dealt with by insurers initiate from open RDP ports. If a company's Remote Desktop Protocol is not absolutely necessary, we would expect it to be turned off. And if RDP is something that is needed, we recommend that it is secured behind a virtual private network and multi-factor authentication.

6

Patch and Patch

Having an inventory of software and hardware assets is an important first step. Once an inventory is established, using a patch management solution will automate most operating system, firmware, and software updates. This reduces the time and resources needed to fulfill this control. These updates can also be undertaken manually when prompted.

7

Endpoint detection

Every device connected to the internet in your business is an "endpoint." Because these points are connected to the internet, they are a potential source of entry for hackers. Endpoint protection software helps secure your computers, tablets, smartphones, and IoT devices against sophisticated malware and wider cyber security threats to the business.