Ascend Broking Group
Business Insurance Solutions

Cyber Breach & Cyber Liability

Cyber Insurance
Who is the risk?

If your business is targeted by a hacker or suffers a data breach, it takes time and money to fix. This can disrupt your business, lead to lost revenue, a damaged reputation **and regulatory fines.**

The continued rise in the amount of information stored and transferred electronically has resulted in a remarkable increase in the potential exposures facing businesses. Regulations, such as the Data Protection Act must also be considered, because a loss of sensitive personal information may subject you to fines and sanctions from the Information Commissioner.

In an age where a stolen laptop or hacked account can instantly compromise the personal data of thousands of customers or an ill-advised post on a social media site can be read by hundreds in a matter of minutes, protecting yourself from cyber liabilities is just as important as some of the more traditional exposures businesses account for in their general commercial liability policies

Cyber Breach & Liability Insurance has become a business necessity.

Cyber Insurance at a glance?

You may need cyber risk cover if:

- You hold customer, supplier or employee information, like names, addresses, bank details or email addresses
- You use a computer to run your business
- You take card payments or make electronic payments
- You have a website

81% of large corporations and 60% of small businesses suffered a cyber breach.

The average cost of a cyber-security breach is £600k-£1.15m for large businesses and £65k-115k for SMEs.

Ascend Broking Group
Business Insurance Solutions

Ascend Broking Group Ltd
21 Springfield Lyons Approach, Chelmsford Business Park, Chelmsford, Essex CM2 5LB
Tel 01245 449 060 | Email info@ascendbroking.co.uk | Web www.ascendbroking.co.uk

Ascend Broking Group
Business Insurance Solutions

Cyber Breach & Cyber Liability

The continued rise in the amount of information stored and transferred electronically has resulted in a remarkable increase in the potential exposures facing businesses. Regulations, such as the Data Protection Act must also be considered, because a loss of sensitive personal information may subject you to fines and sanctions from the Information Commissioner.

Our policy can cover:

Business/Network Interruption

If your primary business operations require the use of computer systems, a disaster that cripples your ability to transmit data could cause you or a third party that depends on your services, to lose potential revenue.

Server failure to a data breach

Such an incident can affect your day to day operations. Time and resources that normally would have gone elsewhere will need to be directed towards the problem which could result in further losses. This is especially important as denial of service attacks by hackers have been on the rise.

Intellectual property rights

Your company's online presence, whether it be through a corporate website, blogs or social media, opens you up to some of the same exposures faced by publishers. This can include libel, copyright or trademark infringement and defamation, among other things.

Human errors

When mistakes made by staff or suppliers result in a data breach.

Damages to a third-party system

If an email sent from your server has a virus that crashes the system of a customer or the software your company distributes fails, resulting in a loss for a third party, you could be held liable for the damages.

System Failure

A natural disaster, malicious activity or fire could all cause physical damages that could result in data or code loss.

Cyber Extortion

Hackers can hijack websites, networks and stored data, denying access to you or your customers. They often demand money to restore your systems to working order. This can cause a temporary loss of revenue plus generate costs associated with paying the hacker's demands or rebuilding if damage is done.

Reputational damage

Arising from a breach of data that results in loss of intellectual property or customers.

Visit www.ascendbroking.co.uk/cyber-data-insurance

Optional extras:

- Financial crime and fraud: When cyber criminals use the internet to steal funds, impersonate your business or deceive employees into transferring money or goods.
- Property damage: Where an incident has caused physical damage to equipment or property, we cover the costs to repair or replace these.
- Dependent business interruption: Where there is a loss of revenue or increased costs incurred when a supplier's systems are taken offline by a cyber incident.

Ascend Broking Group Ltd
21 Springfield Lyons Approach, Chelmsford Business Park, Chelmsford, Essex CM2 5LB
Tel 01245 449 060 | Email info@ascendbroking.co.uk | Web www.ascendbroking.co.uk

Market leading cover

- **Future proofing +**

  One of the four policy triggers is Cyber attack which is defined as 'any digital attack designed to disrupt access to or the operation of a computer system.

  How will it benefit? You can have comfort knowing that your cyber policy is future proofed and will not only respond to attacks known in the current times, but an attack which could be developed in the future which is designed to disrupt their system.

- **Dedicated cyber claims handlers+**

  We have a dedicated team of legally qualified cyber claims handlers to assist you and the client in the event of an incident. A lot of insurers completely outsource the claims handling to a third party .

- **Directors' personal cover**

  Directors who incur personal loss are covered as standard for all cover taken up by the main insured.

  How will it benefit? Directors' want to know their whole business is covered, including their own cyber losses, not just the company itself e.g. directors' transferring personal funds to a hacker or having their family photos held to ransom on their family photos held to ransom on their personal laptop.

- **Full GDPR coverage**

  Full GDPR coverage for data breaches, but also alleged breaches of the regulation.

  How will it benefit? Not all regulatory actions commence due to a data breach, there could be alleged breaches of GDPR which result in a regulatory investigation and this could be particularly pertinent for clients that hold significant amounts of personal data.

- **24/7/365 hotline**

  We will provide a 24 / 7 / 365 response line that the client can call anytime of day / week / year.

  How will it benefit? Would the MD / CEO know who to contact if something like this happens? Given the data held on individuals, they also need to be mindful of the 72 hour reporting requirements under GDPR. Would they know how to do this and investigate the breach within 72 hours and draft an appropriate response to the regulator without assistance?

- **CyberClear Academy**

  Access to a free cyber training platform if they go ahead which educates staff.

  How will it benefit? Insurers will reduce the excess by GBP 2,500 if 80% of networked employees complete the training which can be substantial for a small business. Completion of this training can also be used as evidence that the client has understood and thought about data security risks in the event there is a breach.

Ascend Broking Group Ltd
21 Springfield Lyons Approach, Chelmsford Business Park, Chelmsford, Essex CM2 5LB
Tel 01245 449 060 | Email info@ascendbroking.co.uk | Web www.ascendbroking.co.uk