Gallagher

Insurance | Risk Management | Consulting

Cyber Liability Insurance

Think it won't happen to you?

According to a government report,[1] almost 40% of UK businesses reported having cybersecurity breaches or attacks. Many small businesses may feel it is no longer a question of if they might suffer a breach, but when.

What is Cyber Liability Insurance?

If a company's IT security is found to be inadequate and a breach occurs, the penalties can be high. Cyber liability insurance provides cover for a business for specific liabilities arising out of cyberattacks such as hacking, unintentionally transmitting a computer virus or the failure to properly manage and control personal information. Under the General Data Protection Regulation that came into force in May 2018, you are required to notify your customers of a cybersecurity breach and could be fined up to 4% of your annual turnover.[2]

In addition to potentially substantial fines, it can also lead to a damaged reputation, legal costs, and associated business disruption and lost revenue. Will your customers trust you after a security breach?

Cyber cover and why you may need it

Cyber liability has become headline news following a number of high-profile hacking cases which has led to a greater awareness of the risks and need for cover, but it's not just the large corporates who are at risk. As a managing agent, you are likely to hold a lot of personal and sensitive data concerning your customers. The increasing use of online portals could give hackers access to sensitive information held about individual customer accounts. You can find out more about personal and sensitive data on the Information Commissioner's Office website www.ico.org.uk.

Gallagher works with well-known insurers who offer comprehensive cyber insurance. This is designed to cover you against financial losses and third-party liabilities up to the limits chosen arising from cyberattacks.

Your business is at risk if you:

- Are reliant on computer systems to conduct your business
- Have portals on your website
- Hold sensitive customer data electronically
- Have a transactional website
- Are subject to Payment Card Industry (PCI) merchant and service agreements

Cyber Liability Insurance covers*:

- Liability arising out of media exposure as a result of hacking. For example defamation, libel and infringement of intellectual property rights
- The costs incurred, and which cannot be recouped, as a result of a third party benefitting from a data breach
- Liability arising from the failure to properly handle, manage, store, destroy or otherwise control personally identifiable information
- The costs to withdraw or alter data or images, or other website content as a result of a court order or to mitigate a claim
- Liability arising out of the unintentional transmission of a computer virus
- The costs to recover your computer system records that have been lost, damaged or deleted
- Liability arising out of a hacker's fraudulent use of information
- Compensation costs arising as a result of directors, partners and employees attending court in connection with a covered claim
- Legal defence costs

Cover options available and their benefits*:

1 Forensic costs

Payment for:

- A forensic consultant to establish the identity or methods of the hacker, or any other details required by the insurer following a data breach
- A security specialist to assess your electronic security and reasonable costs to improve them
- The temporary storage of your electronic data at a third-party location, if your information and communication assets remain at risk from a hacker

2 Information and communication recovery costs

- The costs to repair, restore or replace affected parts of your information and IT hardware and software, after they've been stolen, destroyed or affected by a hacker

3 Credit monitoring

- Payment for credit monitoring services in order to comply with data breach law

4 Data breach notification costs

- Costs to inform your customers and anyone affected that a data breach has occurred
- Legal fees incurred to develop notification communications for the affected parties
- The costs to send and administer notification communications
- The costs of call centre services to respond to enquiries and queries following a notification communication

5 Regulatory defence and penalty costs

- Payment for any compensation which you are legally obliged to pay (including legal and defence costs)

6 Cyber business interruption cover

- Payment for loss of income as a result of total or partial interruption of communication assets caused by data security breaches, computer viruses and attacks

7 Cyber extortion

- Payment for reasonable and necessary expenses incurred, including the value of any ransom paid by the insured, for the purpose of terminating a cyber-extortion threat

8 Hardware

- Cover applies to hardware while it is temporarily removed from the insured location
- You can also choose to cover portable hardware anywhere in the world

9 Viruses

- The cost to remove viruses and for specialist advice to prevent viruses or hacking attacks following an incident

If you openly demonstrate weakness in your approach to cybersecurity by failing to do the basics, you may put yourself at risk of a cyberattack.

Every organisation is a potential victim

All organisations have something of value that is worth something to others.

As part of your risk management process, you should be assessing whether you are likely to be the victim of a targeted or untargeted attack. Every organisation connected to the internet should assume they could be a victim of the latter.

Either way, you should implement basic security controls consistently across your organisation, and where you may be specifically targeted, ensure you have a more in-depth, holistic approach to cybersecurity.

Where to go for more help

If you have any doubts or concerns over your cybersecurity or you suspect you might be a victim of cybercrime contact www.actionfraud.police.uk or call the Action Fraud team on 0300 123 2040. Action Fraud is the UK's national fraud and cybercrime reporting centre and provides advice on fraud and cybercrime.
Other sites you may find helpful include www.getsafeonline.org and www.gov.uk/government/collections/cyber-security-guidance-for-business.

Report a crime

To report a nonurgent crime please call your local police on 101. You can also report crime anonymously by calling 0800 555 111. If you are reporting a crime that is in progress or if someone is in immediate danger call 999.

National Crime Agency (NCA) general enquiries

For general enquiries or to verify a person as an NCA officer:
Email: communication@nca.gov.uk
Telephone: 0370 496 7622 (available 24/7)

Cyber threats

The most common types of cyber threats are:

Hacking—including social media and email passwords

Phishing—bogus emails asking for security information and personal details

Malicious software—including ransomware through which criminals hijack files and hold them to ransom

Distributed denial of service (DDOS) attacks against websites—often accompanied by extortion

How secure are you?

You can read the government's cybersecurity guidance for businesses online at

www.ncsc.gov.uk/section/information-for/small-medium-sized-organisations.

*A broad range of cyber cover protection is offered and specialist advice at a time convenient to you. As with all insurance policies, the policy is subject to limits, conditions and exclusions. For full terms and conditions, please refer to the policy wording available on request. This document does not purport to be comprehensive or to give legal advice. While every effort has been made to ensure accuracy, Gallagher cannot be held liable for any errors, omissions or inaccuracies contained within the document. Readers are always recommended to take further professional advice before making any decisions.

Would You Like to Talk?

T: 0800 092 9394

E: UKinfo@ajg.com

[1]www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022
[2]https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/

Gallagher

Insurance | Risk Management | Consulting