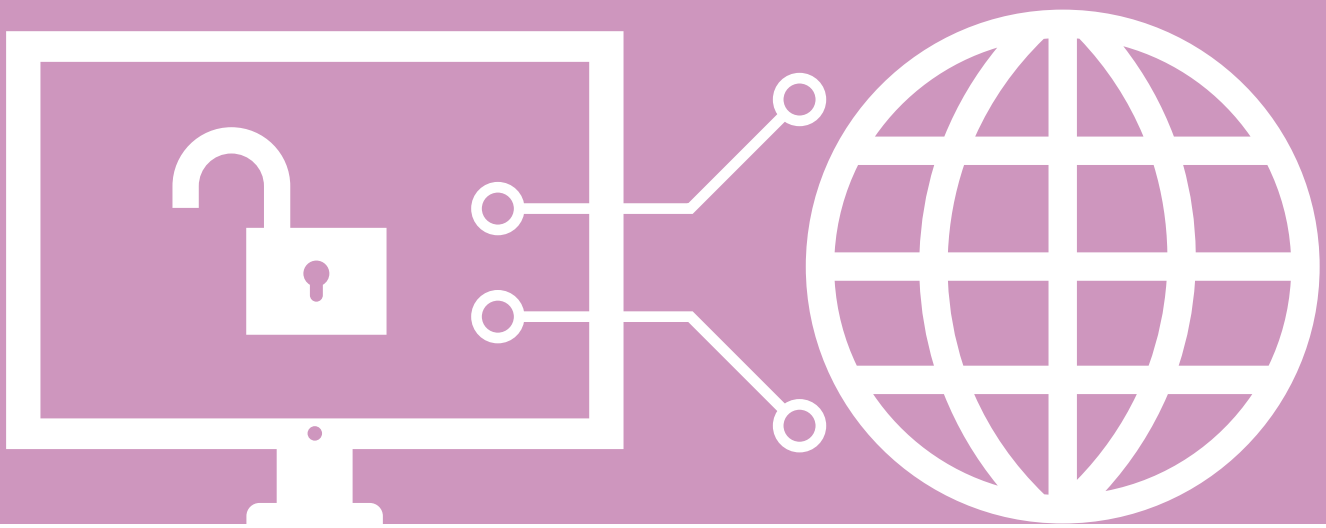
Cyber attacks

Think it won't happen to you?

According to a government report, almost half of businesses (46%), reported having cyber security breaches or attacks in 2020. 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. Under the General Data Protection Regulation that came into force in May 2018, you are required to notify your customers of a cyber security breach and could be fined up to 4% of your turnover**.

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?

0800 149 9564
www.deacon.co.uk

THREE DECADES STRONG · 30 YEARS · ANNIVERSARY

DEACON
Blocks of Flats Insurance

Follow us on

*Official Statistics_Cyber Security Breaches Survey 2020
https://www.gov.uk/government/publications/cyber-security-breaches-survey-2020/cyber-security-breaches-survey-2020.

** The EU General Data Protection Regulation (GDPR)
https://www.itgovernance.co.uk/dpa-and-gdpr-penalties#:~:text=The%20UK%20GDPR%20and%20DPA,whichever%20is%20greater%20%E2%80%93%20for%20infringements.

Cyber cover and why you 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 at the Information Commissioner's Office. www.ico.org.uk

Deacon works with well-known insurers who offer competitive and comprehensive cyber insurance. This covers you against financial losses and third party liabilities up to the limits chosen arising from cyber attacks.

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, data security and multimedia cover

- 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 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*

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

Credit monitoring

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

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

Regulatory defence and penalty costs

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

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

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

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

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

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 cyber security by failing to do the basics, you may put yourself at risk of a cyber attack.

Every organisation is a potential victim*

All organisations have something of value that is worth something to others. If you openly demonstrate weaknesses in your approach to cyber security by failing to do the basics, you may experience some form of cyber attack*.

As part of your risk management process, you should be assessing whether you are likely to be the victim of a targeted or un-targeted 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 cyber security.

Where to go for more help...

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

Report a crime
In an emergency always call 999.

To report a non-urgent crime please call your local police on 101. You can also report crime anonymously by calling 0800 555 111.

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 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 Cyber Security Guidance for Business online at

https://www.gov.uk/government/collections/cyber-security-guidance-for-business

0800 149 9564
www.deacon.co.uk

THREE DECADES STRONG 30 YEARS ANNIVERSARY

DEACON
Blocks of Flats Insurance

Deacon is part of Gallagher, a global insurance, risk management and consulting services company, offering more than 90 years' experience to clients in 150 countries.

Gallagher
Insurance | Risk Management | Consulting

Deacon is a trading name of Arthur J. Gallagher Insurance Brokers Limited, which is authorised and regulated by the Financial Conduct Authority.
Registered Office: Spectrum Building, 7th Floor, 55 Blythswood Street, Glasgow, G2 7AT.
Registered in Scotland. Company Number: SC108909

FP89-2021_11967