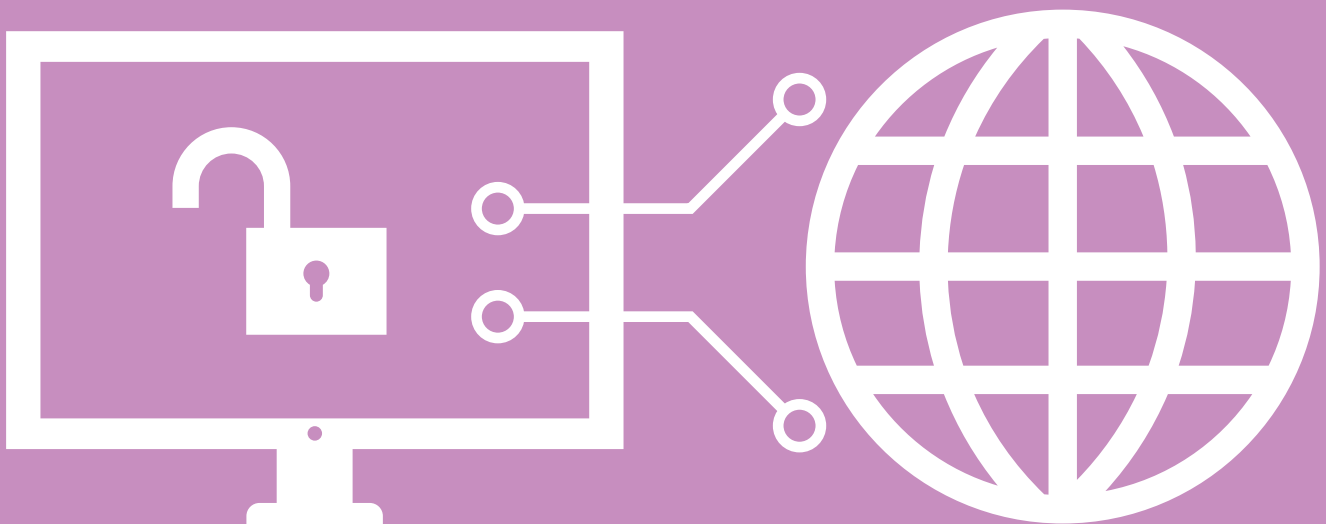
Cyber attacks

Think it won't happen to you?

According to a 2017 government report, there's around a 1 in 2 chance that small businesses (SMEs) will experience a cyber security breach. 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 EU regulations coming into force 25 May 2018, you will be 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?

0808 149 9564
www.deacon.co.uk

DEACON
Blocks of Flats Insurance

Follow us on

*The Department for Digital, Culture, Media and Sport's 'Cyber Security Breaches Survey 2017' reported that just under half (46%) of all businesses have identified at least one cyber security breach or attack in the last 12 months (and 38% have among micro-firms, 52% have among small firms and 66% have among medium firms).

** The EU General Data Protection Regulation (GDPR)
https://www.itgovernance.co.uk/data-protection-dpa-and-eu-data-protection-regulation

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

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. ActionFraud 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.

"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.

TalkTalk, Yahoo, PlayStation, the AA and Three

Evening Standard 6 December 2017**

It's not just the big players that suffer cyber-attacks, but when they do it makes headline news. Research published in December 2017 suggest that millions of British victims of data breaches are unaware their personal data has been stolen. About 30 high-profile hacks over the past two years were analysed, including Talk Talk, Yahoo, PlayStation, the AA and Three, with researchers calculating up to 77 per cent of Britons had fallen victim to cybercriminals. And that was before the hacks at Uber and Equifax at the end of 2017. Personal information taken by hackers, which often ends up for sale on the dark web, has included names, addresses, phone numbers, bank account details and passwords. An overhaul of data protection laws this year (GDPR May 2018) will mean companies will need to tell customers if there has been a significant data breach. Firms in the UK that suffer a serious breach could be fined up to £17M or 4% of turnover of the previous financial year.

** https://www.standard.co.uk/news/techandgadgets/millions-unaware-their-personal-details-were-hacked-in-recent-cyber-attacks-study-says-a3712051.html

SMEs more vulnerable than ever to cyber attacks, survey shows

Computer Weekly 16 October 2017†

The biggest cyber threat to UK and US small businesses is employees' weak passwords, as the frequency, intensity and cost of cyber attacks continue to rise, a study has revealed. The overwhelming majority of cyber attacks on small to medium-sized enterprises (SMEs) result from poor password management and employee negligence, a study of 1,000 UK and US SMEs by the Ponemon Institute.

According to the survey 61% of respondents reported a cyber attack, up from 55% a year ago – while 54% reported a data breach, up from 50% a year earlier. Ransomware attacks were reported by 52% of respondents, with 53% of those reporting they were hit by more than one ransomware attack.

The total costs associated with successful cyber attacks on SMEs now total well in excess of £1M, meaning a single attack could bring an SME to it's knees financially.

† http://www.computerweekly.com/news/450428246/SMEs-more-vulnerable-than-ever-to-cyber-attacks-survey-shows

* From Common Cyber Attacks: Reducing the Impact, from the CESG The Information Security Arm of GCHQ https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/common_cyber_attacks_2016.pdf

0808 149 9564
www.deacon.co.uk

DEACON
Blocks of Flats Insurance

FP1042_2017_Exp Jan 2019_9060