Everything you need to know about cyber insurance

tmd
insurance group

Chartered
Insurance
Brokers

Cyber insurance
What is it and do you need it?

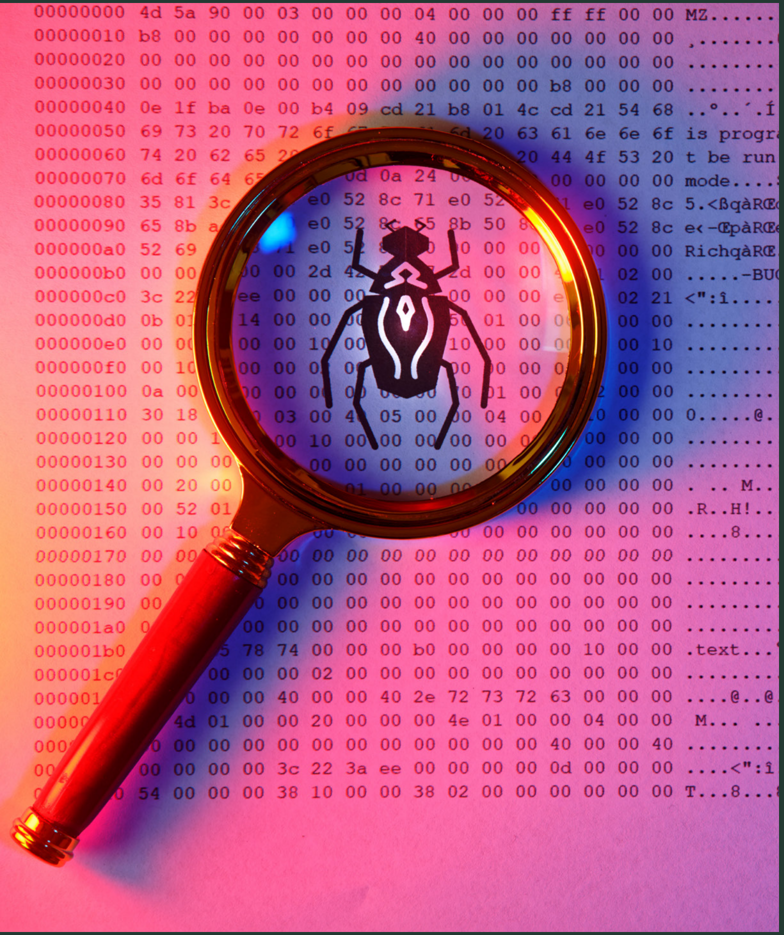
Technology has revolutionised the world in which we live. For businesses, it has brought unprecedented opportunities in terms of innovation, efficiency, speed and scale. But it has also created new exposures and introduced the risk of cybercrime.

With organisations more connected than ever and increasingly dependent on technology, every business must take steps to manage the risk of cybercrime proactively.

It's true that cyber criminals target organisations of all sizes and across all sectors, but it's the small businesses that often lack the security and technical expertise of larger companies and are unprepared to withstand an incident. As a result, thousands of smaller businesses suffer cyber incidents each year.

FACT The biggest cyber risk is complacency, not hackers

96% of all cyberattacks are directed at small & medium-sized businesses



In the last few years, cyber insurance has become more technically-led and service-oriented, aiming to prevent cyber incidents from happening and respond quickly if they do.

The core components of a good cyber insurance policy include:

→ Financial loss arising from a cyber event

→ Liability actions by third parties due to a cyber event

→ 24/7 proactive services to prevent a cyberattack from happening

→ Incident response services to get systems and networks up and running after a cyberattack

FACT

39% of UK companies have reported a data breach incident to the Information Commissioner's Office (ICO) in the last 12 months.*

How would you react in the event of a cyberattack?

If you're not sure whether you need cyber insurance, ask yourself how you would react in the following circumstances:

1 You come into work and find that someone has got into your system and accessed your data. What would you do?

2 Someone hacks into your business and puts messages out on social media. How do you stop them and repair the reputational damage?

3 You switch on your computer and there is no response, just a ransom demand. Would you pay? Who would you call? What would you say to customers and employees?

If your system is compromised, paralysed or attacked, cyber insurance protects your business against reputational and financial damage and helps you meet your commitments to customers, employees and the Information Commissioner's Office.

*Cyber Security Breaches Survey 2022 ICO/GOV.UK

Cyber misconceptions

As cyber is now one of the largest exposures for any business, it's important to overcome some popular misconceptions and highlight the true value of cyber insurance.

We outsource our IT, so we don't have exposure.

Using a third party for IT doesn't eliminate your exposure. If you outsource your data storage to a third party and they are breached, you are still responsible for notifying affected individuals and dealing with regulatory actions. If you rely on a third party for business-critical operations and they experience a system failure, it could have a catastrophic effect on your ability to trade.

We don't need cyber insurance. We invest in IT security.

No matter how much a company spends on IT security, it can never be 100% secure. The cyber landscape is ever-changing and cyber threats continually evolve: even large corporations that spend vast amounts on cyber security routinely get hit. Theft of funds, ransomware, extortion and data breaches usually start with human error or oversight, allowing cybercriminals to access your systems. Cyber insurance adds another layer of protection and response in the event of an attack.

Cyber misconceptions (continued)

We don’t collect sensitive data, so we don’t need cyber insurance.

You don’t need to collect sensitive data to have cyber exposure. Any business that relies on a computer system to operate has very real cyber exposure. Two of the most common and costly sources of cyber claims are ransomware and funds transfer fraud, neither of which involves a data breach, but both can lead to severe financial losses, which are insurable under a cyber policy.

Cyber is covered by other lines of insurance.

Cyber cover in traditional lines of insurance often falls short of the cover found in a standalone cyber policy, and some policies have a ‘total’ cyber exclusion clause. Property policies were designed to cover your bricks and mortar, not your digital assets, and liability policies don’t usually cover first-party costs associated with a cyber event. A standalone cyber policy comes with access to expert handlers who are trained to get your business back on track with minimum disruption and financial impact.

What is cybercrime?

Cybercrime is ever-evolving and becoming increasingly sophisticated, taking many different forms:

Phishing or social engineering: Is an attempt to dupe your business into transferring funds to criminals or provide sensitive information as a result of fraudulent emails purporting to come from employees, directors, customers or suppliers.

Ransomware, cyber extortion and malware attacks: A threat actor encrypts and disables access to your business-critical systems and data until a ransom payment is made. If the ransom isn't paid, data may be exfiltrated and exposed.

Business email compromise: Email intrusion resulting from spoofing, phishing or spear phishing can result in a data breach or funds transfer loss.

Funds transfer fraud (FTF): Social engineering or phishing causes funds to be sent to the attacker instead of the proper recipient.

Web application compromise: Direct compromise of web-based technology, such as an e-commerce platform, as a result of a cyberattack.

Data breaches: A security incident exposes confidential or protected information, either due to a security failure or instigated by a cyberattack.

Legal and regulatory issues: Violation of legal or regulatory framework, such as GDPR, HIPAA, PIPEDA or CCPA.

Technology Errors & Omissions (E&O): Failure in the technology product or servicing, resulting in business interruption or loss on behalf of your customers.

What does cyber insurance do?

A cyber insurance policy brings together cyber security, in-depth technology and insurance expertise to help you assess, prevent and respond to the emerging risk of cyberattack. It provides a holistic approach, offering support before, during and after an incident in the form of risk assessment, protection and response. Most policies can be tailored to meet your individual risk profile and can cover:

→ Hackers stealing data and demanding a ransom not to release it

→ Viruses that paralyse systems, and the income lost while the systems are restored

→ Accidental loss of data and subsequent third-party litigation

→ Financial payments, transfer of securities or property made by you in direct response to social engineering communication

→ Use of the Internet to deceive employees, customers or suppliers into transferring money or goods

FACT Cyber criminals target companies who are vulnerable rather than valuable.

The core components of cyber cover:

Costs involved: The cost of removing a virus or malware, notifying affected customers, credit monitoring and bringing in forensic teams.

Damage to data or programming: The cost of restoring affected data or security programmes.

On-site network failure: Covers business interruption losses arising as a result of the breach or network failure. (In respect of own on-site network failure. Hosted network failure is an optional extension).

Multimedia liability: Breach of copyright, libel or slander, plagiarism or defamation if you are sued as a result of information appearing on business account social media pages, such as Twitter or Facebook.

Regulatory: Legal costs are incurred if you have to comply with regulatory action taken as a result of a breach.

Cyber extortion / ransomware: The costs of any extortion or ransomware payments associated with the attack (costs will not be paid if known to be funding terrorism).

Network security, privacy and confidentiality liability: Covers your liability if you are sued by affected customers, vendors or employees in the event of a data breach.

Cyber Terrorism: Losses caused by individuals, groups or governments acting for political, religious or ideological purposes, causing disruption of your computer systems.

Payment card industry: Fines incurred due to failure to follow PCI security standards properly.

Company Registration Number: 02856600
FCA Registration Number: 307258.
TMD Insurance Group is a trading style of Tony McDonagh & Co Ltd which is authorised and regulated by the Financial Conduct Authority (FCA).

Why you can trust TMD

TMD is one of the UK's largest independent insurance brokers, with a team of knowledgeable advisors highly experienced in managing risk and arranging cyber insurance. Established in 1971, we have grown consistently over the decades, with the majority of our customers renewing year on year.

Fiercely proud of our independent status, we aim to deliver key benefits to customers, and as a Chartered Insurance Broker, work consistently to the highest professional standards. Totally committed to your wellbeing, our business is your protection.

To find out more about cyber insurance and how it can protect and benefit your business, please don't hesitate to get in touch.

Contact us:
Telephone: 01992 703000
Email: insurance@mcdonaghs.co.uk
www.tmdinsurance.co.uk

Chartered Insurance Brokers

tmd
insurance group