Everything you need to know about cyber insurance.

tmd insurance group

What is cyber insurance and do you need it?

There's a lot of confusion about cyber insurance and whether you need it. This brochure is designed to answer some of your questions.

To start with, ask yourself which part of your business is not reliant on a digital system. If a cyber attack meant this was the only functioning part of your business, what could you do?

The answer is, probably, not much.

That's what cyber insurance is for, to keep your business running in a world operated by digital systems and increasingly threatened by cyber attack.

To put cyber threat into perspective, up to 88% of UK companies have suffered breaches in the last 12 months.

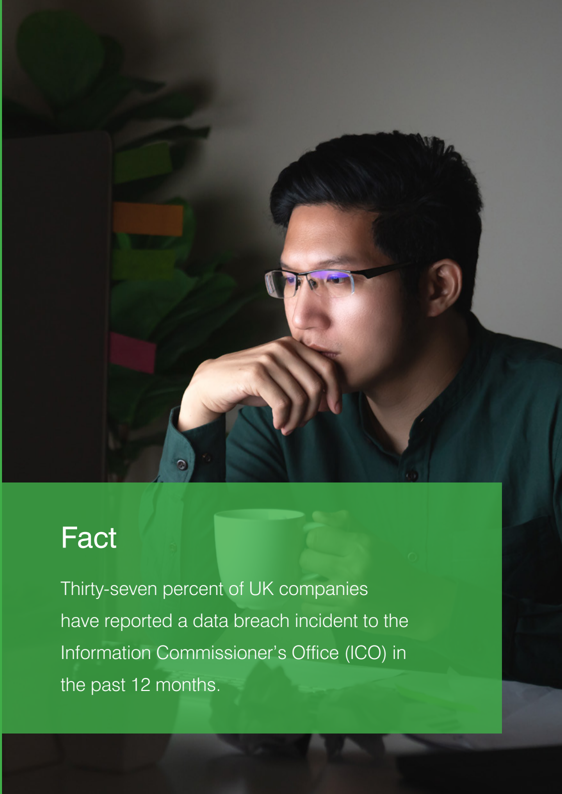
Fact

Around 65,000 attempts to hack SMEs occur in the UK every day, around 4,500 of which are successful.

How would you react in the following circumstances?

1. You come into work and are told that someone has got into your system and accessed your data. What would you do?
2. Someone hacks your business and starts putting out messages on social media. How do you stop them and repair the reputational damage?
3. You switch on your computer and there is no response, except for a ransom demand. Who would you call, and would you pay? What would you say to your customers and employees?

Cyber insurance tackles these threats and more. If your digital system is compromised, paralyzed or attacked, it protects your business and helps you meet your commitments to customers and employees.

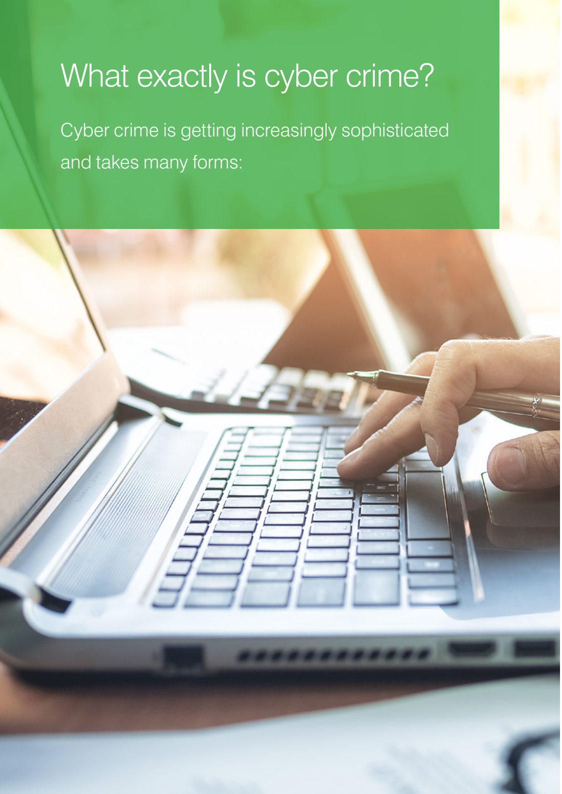


Fact

Thirty-seven percent of UK companies have reported a data breach incident to the Information Commissioner's Office (ICO) in the past 12 months.

What exactly is cyber crime?

Cyber crime is getting increasingly sophisticated and takes many forms:



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

Whaling is an attempt to land a big fish, such as a CEO, with a sophisticated scam, such as paying a large sum for a fake acquisition.

Hacking is where a hacker gets into your business files or server and gains information.

Cyber extortion is where a hacker enters your computer and disenables your business files, demanding a ransom, usually in Bitcoin, to reinstate them.

DoS Attack is an attempt to bring a website or network to a standstill by flooding it with data requests.

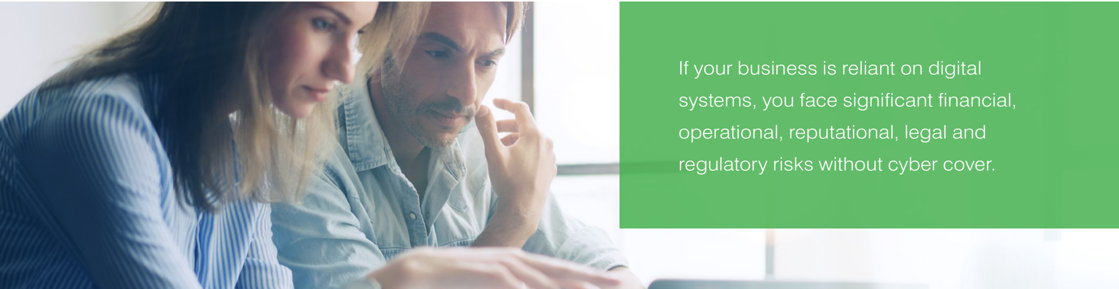
Virus is a small program designed to cause trouble by gaining access to your device, it usually self-replicates after hooking into your system.

Malware is a general term for malicious software, such as WannaCry and NotPetya. It can include ransomware, spyware, worms and Trojans.

What does cyber insurance do?

A cyber insurance policy can be tailored to your business's individual risk profile, covering:

- Hackers stealing data and demanding a ransom not to release it
- Viruses that paralyse systems, and the income lost while they are being restored
- Fines and penalties you may occur if you are assessed as being non-compliant with the new GDPR rules and they are insurable in the jurisdiction where such award was first ordered.
- Accidental loss of data, followed by legal action on the part of customers
- The transfer by you of your money, securities or property in direct response to a social engineering communication
- Use of the internet to deceive employees, customers or suppliers to transferring money or goods



If your business is reliant on digital systems, you face significant financial, operational, reputational, legal and regulatory risks without cyber cover.

Core components of cyber cover:

The cost of removing a virus or malware, notifying affected customers, offering 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 result of breach or network failure. (This is in respect of own on site network failure – hosted network failure is an optional extension).

Regulatory
Legal costs 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 wouldn't 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.

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.

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 properly follow PCI security standards.

CONTACT

If you require any further information about our products or services please contact us on:

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

tmd
insurance group

TMD Insurance Group is a trading style of Tony McDonagh & Co Ltd which is authorised and regulated by the Financial Conduct Authority (FCA).
Company Registration Number: 0856600
FCA Registration Number: 307258