

Resources

# A beginner's guide to cyber insurance



**QMT**COMMERCIAL  
INSURANCE BROKERS

# What is cyber insurance?

Cyber insurance protects businesses financially from the impact of cyber crime and data breaches. Cover typically includes:

## **First Party Losses**

Direct financial loss to your business, e.g. theft of funds, data theft or damage to digital assets.

## **Third Party Liabilities**

Defence costs, settlement and damages for third party claimants affected by a cyber incident.

## **Incident Response**

Expenses to investigate and recover from a cyber attack, including system repairs and data restoration.

## **Business Interruption**

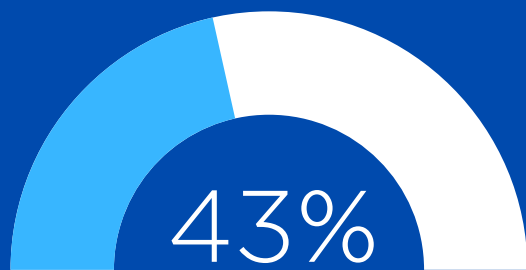
Cover for lost income due to downtime or disruption caused by a cyber breach.

## **Data Breach Notification**

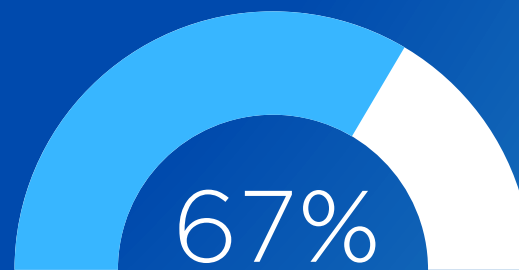
Costs associated with notifying customers or regulators about a data breach, including legal fees and public relations.



# How common are cyber risks?



of businesses reported a cyber security breach or attack in the last 12 months



of medium sized businesses reported a cyber security breach or attack in the last 12 months

£3,550

the average cost of the most disruptive breach (excluding those with no costs)

4 IN 10

businesses taking part in the survey reported having no cyber insurance in place



# Types of cyber security breaches

There are many cyber risks, including:

## **Malware**

“Malicious software” designed to harm computer systems, networks or devices, including viruses, ransomware and spyware.

## **Ransomware**

A type of malware that encrypts the victim's personal data until a ransom is paid.

## **Phishing**

A criminal tactic using emails disguised as legitimate communications to trick victims into revealing sensitive information.

## **Email Hijacking**

Where the hacker gains access to a target's email account and uses the information for malicious purposes.

## **Spoofing**

Where someone pretends to be another entity to gain unauthorised access, steal information or spread malware.

# What steps can be taken to prevent cyber crime?

Update your processes to have a policy for identifying and dealing with phishing emails and another policy for using strong passwords.

Ensure you are using up to date malware and antivirus protection.

Restrict admin rights.

Network firewalls.

Backup data to the cloud.

# What else can you do?

In today's digital landscape and with emerging AI technology, it is impossible to eliminate all cyber risks. Therefore, every business should consider adding cyber insurance to their existing insurance arrangements.



# Need help with your insurance?

Our team of friendly advisors  
are here to support you, whether  
you need a quote or have a query.

01227 285 540

HEAD OFFICE

01233 222 562

ASHFORD BRANCH

Find more tips and resources:  
[www.qmtcommercial.co.uk/hub](http://www.qmtcommercial.co.uk/hub)