

CONCORDE

INSURANCE BROKERS LTD

CYBER INSURANCE

Protect your business from cyber threats

Insurance provided by:

BEWICA



We protect you against the threats of a digital world

If you suffer a loss from a cyber attack or data breach, Bewica cyber insurance helps your business get back up and running as soon as possible.

What we cover you for



Hacking

page 3



Data breaches

page 4



Other data liability

page 5

How we protect you



Pay out for your costs or damages

page 6

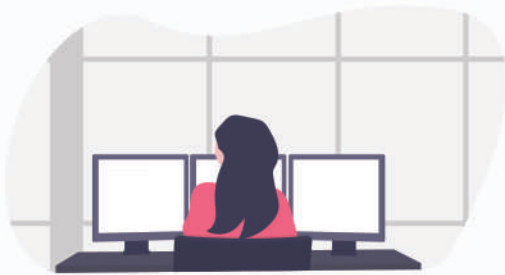


24/7 breach response hotline

page 7

Hacking

Unauthorised systems access or usage

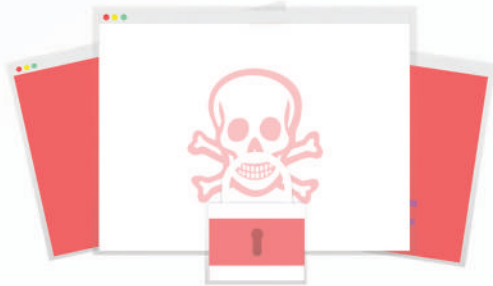


If hackers gain access to your systems or uses your computing resources

Example:

If your business is affected by a computer virus or other malware.

Extortion threat

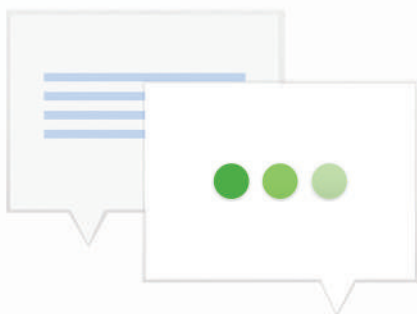


Ransomware and other threats to your data or systems.

Example:

If a hacker encrypts your data and demands a ransom for the key to decrypt the data.

Social engineering



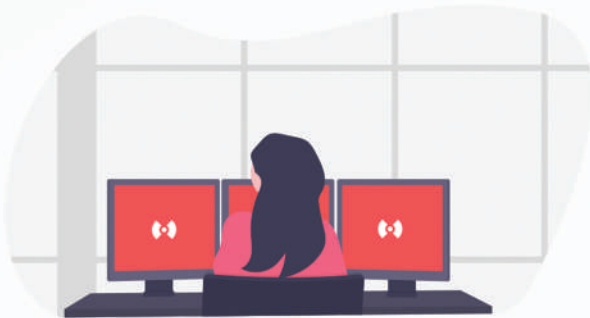
Manipulation by use of website or e-communication to obtain confidential information or money.

Example:

If a criminal tricks an employee into sending them sensitive client data.

Data breaches

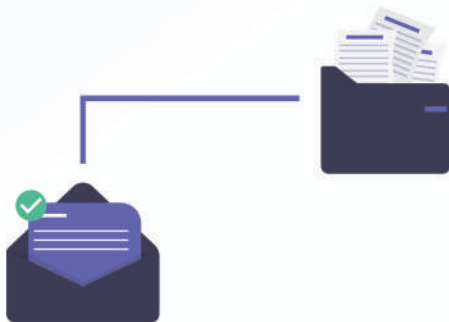
What is a data breach?



A data breach occurs when **confidential information or personal data** is:

- Lost
- Stolen
- Corrupted
- Accessed or disclosed without proper authorisation

Accidental breach example



Wrong Attachment

An employee attaches the incorrect spreadsheet in an email to a supplier.

This spreadsheet contains confidential customer information which this supplier should not have access to.

Intentional breach example



Hacker finds unsecured database

A customer database is left unsecured by a business' technical team.

A hacker finds this database and posts the customer data on social media.

What we cover you for

Other data liability

PCI breach

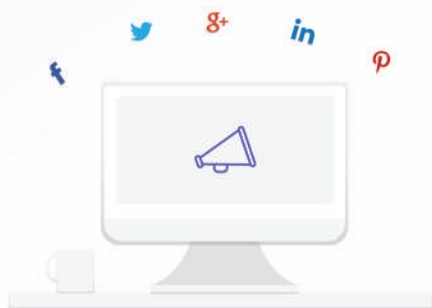


Breach of standards and regulations issued by the payment card industry security standards council.

Example:

If your tech team accidentally leaves an online payment page unsecured

Media event



IP infringement and defamation claims from 3rd parties related to media usage.

Example:

If your social media manager uses a copyrighted image without permission

Privacy breach (GDPR)



Infringement of privacy rights and regulation in regards to personal or confidential data.

Example:

If you fail to notify clients about a data breach involving their information.

Our insurance covers a wide range of costs



Breach expenses

External costs to manage a cyber incident* such as IT forensics, PR, legal costs and credit monitoring.



Extortion monies

Ransomware payments and other costs resulting from a cyber threat.



Business interruption

Loss of income to your business and increased costs of working resulting from a cyber incident*.



Dependent business interruption

Loss of income due to a cyber attack affecting your systems or website provided by an outsourced provider.



Data recovery and data mitigation

External costs to restore damaged or destroyed data and to prevent further damage from a cyber incident*.



Regulatory action

Legal costs to defend and, where insurable by law, any fines or penalties resulting from a cyber incident*.



PCI Fines

Costs and fines arising from a breach in payment card industry data security standards.



Claims against you

Third-party damages and legal defence following a cyber incident or media event*.



Customer loss

Loss of income from damage caused by a cyber incident to your reputation*.



Cyber theft

Loss of money or other financial assets due to a cyber attack.
(Social engineering based theft is an optional cover)

*A cyber incident includes unauthorised systems access or usage, social engineering, data breach or privacy breach.

How we protect you

24/7 breach response hotline



Call our 24/7 breach response hotline if you have a cyber incident or data breach.



Things you might not know about cyber attacks

1. Most businesses, even small ones, experience a cyber attack each year.

Even the best IT teams in the world can't make your business 100% safe from cyber attacks or human error. Our cyber insurance policy acts as a safety net when your other measures fail.

37%

of UK small businesses have experienced a breach in the last 12 months.*

2. The most disruptive attacks on businesses often have nothing to do with websites.

Emails for instance, are used by almost all businesses and are a key attack channel of many hackers. Our research suggests that 94% of employees will receive a phishing email within a 12 month period.

82%

of the most disruptive attacks to UK businesses were unrelated to their website *

3. Financial losses from cyber attacks are larger than you might think

Small attacks are often easy to remediate, but that's not what cyber insurance is for. Cyber insurance is there for when you have an attack that you struggle to recover from and need the financial or expert support to get your business back on its feet.

£20k+

is the cost 1 in 10 businesses will experience if are cyber attacked. *

4. Our cyber insurance has been designed to give businesses strong protection

Bewica cyber insurance is specifically designed to cover a broad range of attacks and incidents. This minimises the chances of a claim not being accepted.

96%

of the most disruptive attacks to UK businesses are covered by a Bewica cyber policy **

* Data from UK Government breaches survey

** Data from UK Government breaches survey and assumes optional cyber theft added to policy.

CONCORDE

INSURANCE BROKERS LTD

Copyright © 2019 Bewica Limited. Bewica Limited is a company registered in England and Wales under company number 10853421. Bewica is authorised and regulated by the Financial Conduct Authority under the registration number 791243. See the Financial Services Register for further details.

Insurance provided by:

BEWICA