cybercovered

Ascend Broking Group
Business Insurance Solutions

PROTECTING YOUR BUSINESS

from cyber and data risks

A business today operates very differently to the businesses from a few years ago. Email, web applications and electronic processeses not only dominate operations but are key in helping businesses keep costs low and ultimately succeeding.

Our cyber & data policy is built to protect you against the cyber risks of todays digital world. If you suffer a data breach or cyber attack, we will get you back up and running - whilst protecting your balance sheet.

We cover you for

Data breaches & Cyber Liability 3-4

Business interruption 5

Legal & regulatory costs 6

Hackers & extortion 7

Cybercrime & telephone hacking 8

How we manage an incident? 9

Cyber facts 10

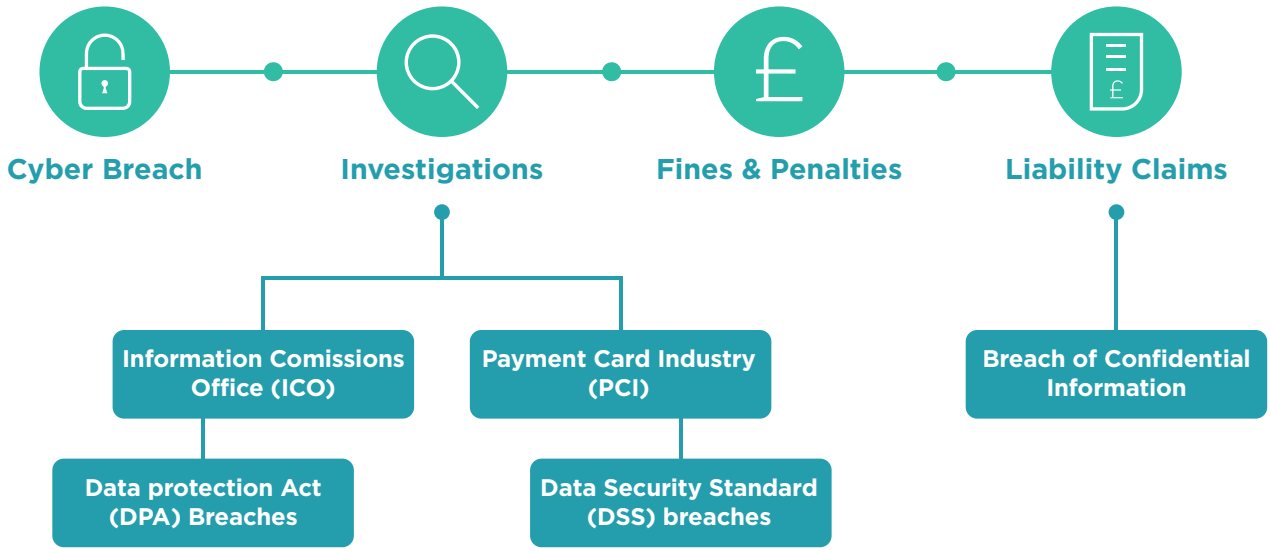
What is a Data Breach

A data breach is when confidential information is:

- Accessed or disclosed without permission
- Lost or stolen
- Corrupted or interfered with

Common types of data comprimised:

- Passwords & Account information
- Credit and personal card details
- Business banking account information
- Medical Records
- Customers Personal Information
- Intelectual property or software source code etc.



Exposure

Any business holding personal information is at risk of a data breach, be it from an external cyber-attack to a simple employee error such as sharing a confidential document with the wrong party or losing a company device.

Online Liability

If a claim is made against you arising from;

- Content of your email,
- Website or online publication.
- Other electronic communications - These can include false emails as a result of alterations made by a hacker

Alternatively, if a claim is made against you for breach of personal data or sensitive commercial information our cyber policy will protect you.

Exposure

Whether it is an employee posting opinions about a competitor or hackers gaining control of your office network to publish altered documentation, the online world creates new forms of liability that can be devastating to a business.

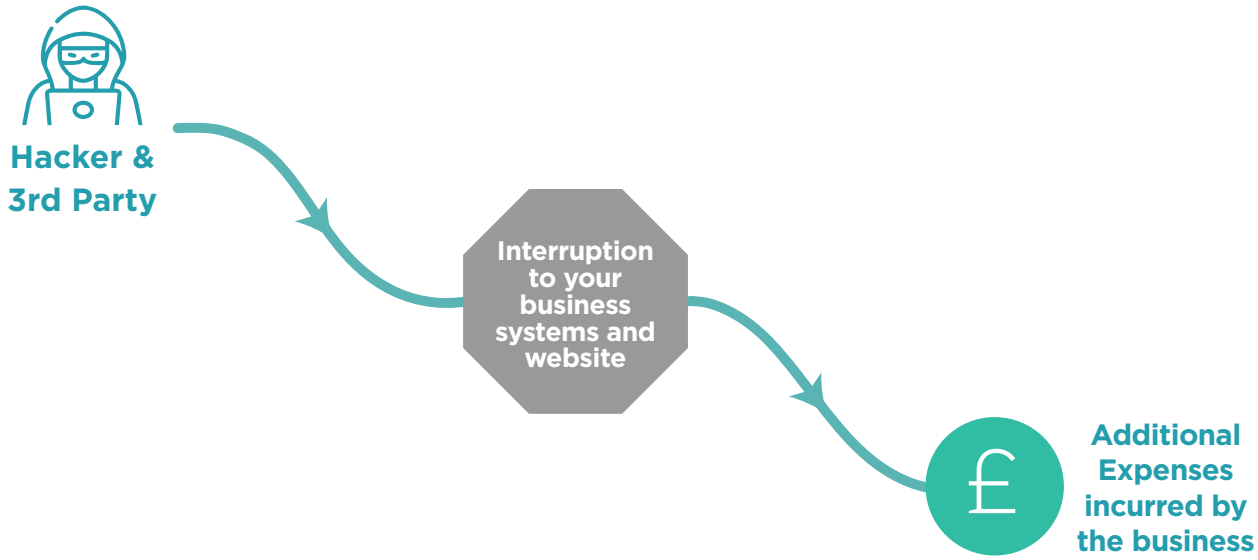
What am I covered for?

Business Interruption

If your business suffers from an interruption as a result of a breach from a third party or a hacker.

The policy will pay for:

- Your loss of income
- Damage to your reputation
- Increased costs of working to the business

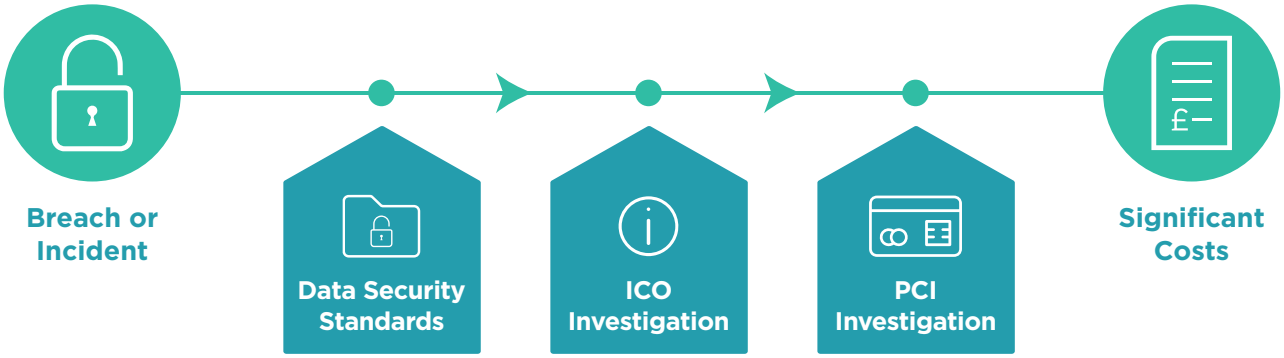


Exposure

An interruption to the IT network or systems can quickly escalate into a threat to a business. From sophisticated external threats, such as ransomware or distributed denial of service (DDoS) attacks on a website, to simple operator error such as unplugging the wrong server or a system crash when updating. Cyber induced business interruption can strike at any time and be very costly to a business.

What am I covered for?

Legal & Regulatory Costs



Following a cyber breach, it is common for the involvement of lawyers and specialists in dealing with the investigating bodies and notifying data recipients, these legal fees can be costly.

The policy will pay for:

- The costs incurred in defending a regulatory investigation or prosecution
- Compensation payable or PCI charges for which you become liable as a result of a breach
- Infringement of intellectual property rights

Exposure

From the costs of complying with a regulatory investigation following the loss of client data, such as the ICO or the PCI (payment card industry), to claims from third parties, legal and regulatory expenses can rapidly escalate following a cyber event.

What am I covered for?

Hackers & Cyber Extortion

If Hackers gain access to your data or systems;

The policy will pay for:

- Putting right any damage, corruption or misuse of your computer systems or programmes that has occurred.
- Recovery of copied or stolen programmes and repairing data held electronically.

Example

1

An email is sent to the admin team with information about the coronavirus and new government schemes.

2

When opened malware is installed into the network and an error message appears on all devices demanding that a ransom of £10,000 be paid in bitcoin to restore access to the network.

3

The organisation would need to first access a specialist IT firm to restore access to the network before conducting a cost benefit analysis of paying the ransom demand.

4

Public relation specialists may be required to manage the message to customers regarding the downtime and its impact to the business.

What am I covered for?

Cyber Crime

If you discover a loss caused by a third party who is not an employee of yours, arising from theft, transfer or corruption of your money.

The policy will pay for:

- Your financial loss of the funds transferred
- The cost of repairing, replacing or reinstating any digital assets or tangible property
- Increased costs of working to the business
- The direct cost to you of any unauthorised telephone call

Example

A manufacturer had agreed to switch material suppliers to a new local vendor.

Following the agreement, the new supplier sent an invoice for the materials.

Two minutes later an email, appearing to be from the same address, advised old banking information, and should be discarded with payment being made to the new details attached.

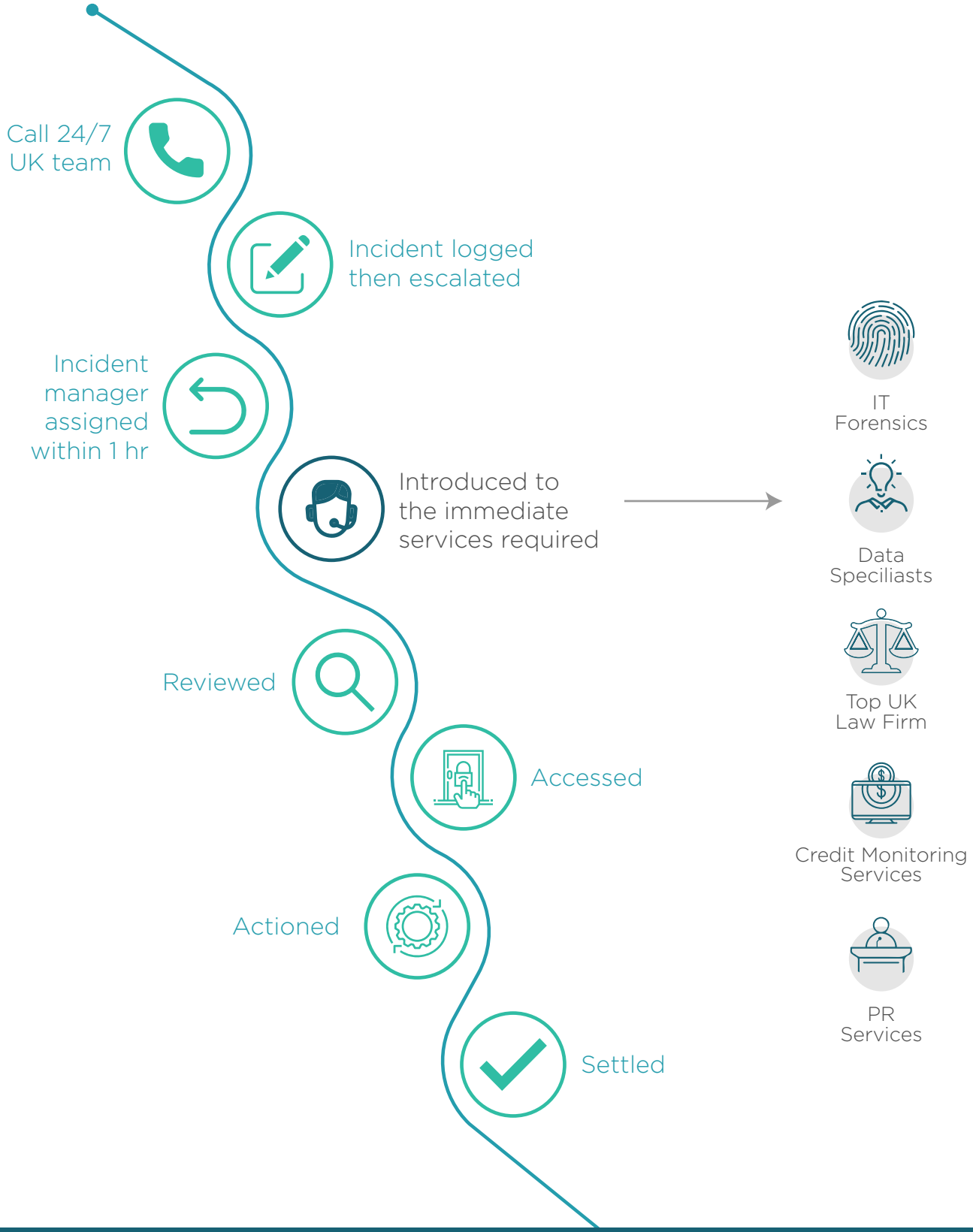
Hackers had gained access to the IT network and were monitoring emails for such a transaction.

Funds were paid

Only noticed that the email address contained an incorrect character once the supplier chased for the payment some weeks later, leaving the firm without the money and still liable for the order.

How we manage an Incident

Our simple process to help you when you most need it:



7 Cyber Facts

88% Up to 88% of UK companies have suffered breaches in the last 12 months

19sec One small business in the UK is successfully hacked every 19 seconds

65k Around 65,000 attempts to hack small to medium-sized businesses (SMBs) occur in the UK every day, around 4,500 of which are successful.

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

17% 17% had reported more than one incident

20% Around half of cyberattacks in the UK involve phishing targeted at SME businesses. That's around 20% higher than the global average.

60% 60% of businesses that suffer a cyber breach without cyber insurance in place, will go out of business within 6 months.

cybercovered

Ascend Broking Group
Business Insurance Solutions

For all Enquiries
please contact:
info@cybercovered.com

Sources

*Carbon black report 2019
*Hiscox study and report 18/19
*CISCO report 2018