Ascend Broking Group
Business Insurance Solutions

Cyber Breach & Cyber Liability

Cyber Insurance
Who is the risk?

If your business is targeted by a hacker or suffers a data breach, it takes time and money to fix. This can disrupt your business, lead to lost revenue, a damaged reputation **and regulatory fines.**

The continued rise in the amount of information stored and transferred electronically has resulted in a remarkable increase in the potential exposures facing businesses. Regulations, such as the Data Protection Act must also be considered, because a loss of sensitive personal information may subject you to fines and sanctions from the Information Commissioner.

In an age where a stolen laptop or hacked account can instantly compromise the personal data of thousands of customers or an ill-advised post on a social media site can be read by hundreds in a matter of minutes, protecting yourself from cyber liabilities is just as important as some of the more traditional exposures businesses account for in their general commercial liability policies

Cyber Breach & Liability Insurance has become a business necessity.

Cyber Insurance at a glance?

You may need cyber risk cover if:

- You hold customer, supplier or employee information, like names, addresses, bank details or email addresses
- You use a computer to run your business
- You take card payments or make electronic payments
- You have a website

81% of large corporations and 60% of small businesses suffered a cyber breach.

The average cost of a cyber-security breach is £600k-£1.15m for large businesses and £65k-115k for SMEs.

Ascend Broking Group
Business Insurance Solutions

Ascend Broking Group Ltd
21 Springfield Lyons Approach, Chelmsford Business Park, Chelmsford, Essex CM2 5LB
Tel 01245 449 060 | Email info@ascendbroking.co.uk | Web www.ascendbroking.co.uk

Ascend Broking Group
Business Insurance Solutions

Cyber Breach & Cyber Liability

The continued rise in the amount of information stored and transferred electronically has resulted in a remarkable increase in the potential exposures facing businesses. Regulations, such as the Data Protection Act must also be considered, because a loss of sensitive personal information may subject you to fines and sanctions from the Information Commissioner.

Our policy can cover:

Business/Network Interruption

If your primary business operations require the use of computer systems, a disaster that cripples your ability to transmit data could cause you or a third party that depends on your services, to lose potential revenue.

Server failure to a data breach

Such an incident can affect your day to day operations. Time and resources that normally would have gone elsewhere will need to be directed towards the problem which could result in further losses. This is especially important as denial of service attacks by hackers have been on the rise.

Intellectual property rights

Your company's online presence, whether it be through a corporate website, blogs or social media, opens you up to some of the same exposures faced by publishers. This can include libel, copyright or trademark infringement and defamation, among other things.

Human errors

When mistakes made by staff or suppliers result in a data breach.

Damages to a third-party system

If an email sent from your server has a virus that crashes the system of a customer or the software your company distributes fails, resulting in a loss for a third party, you could be held liable for the damages.

System Failure

A natural disaster, malicious activity or fire could all cause physical damages that could result in data or code loss.

Cyber Extortion

Hackers can hijack websites, networks and stored data, denying access to you or your customers. They often demand money to restore your systems to working order. This can cause a temporary loss of revenue plus generate costs associated with paying the hacker's demands or rebuilding if damage is done.

Reputational damage

Arising from a breach of data that results in loss of intellectual property or customers.

Visit www.ascendbroking.co.uk/cyber-data-insurance

Optional extras:

- Financial crime and fraud: When cyber criminals use the internet to steal funds, impersonate your business or deceive employees into transferring money or goods.
- Property damage: Where an incident has caused physical damage to equipment or property, we cover the costs to repair or replace these.
- Dependent business interruption: Where there is a loss of revenue or increased costs incurred when a supplier's systems are taken offline by a cyber incident.

Ascend Broking Group Ltd
21 Springfield Lyons Approach, Chelmsford Business Park, Chelmsford, Essex CM2 5LB
Tel 01245 449 060 | Email info@ascendbroking.co.uk | Web www.ascendbroking.co.uk

Market leading cover

- **Future proofing +**

  One of the four policy triggers is Cyber attack which is defined as 'any digital attack designed to disrupt access to or the operation of a computer system.

  How will it benefit? You can have comfort knowing that your cyber policy is future proofed and will not only respond to attacks known in the current times, but an attack which could be developed in the future which is designed to disrupt their system.

- **Dedicated cyber claims handlers+**

  We have a dedicated team of legally qualified cyber claims handlers to assist you and the client in the event of an incident. A lot of insurers completely outsource the claims handling to a third party .

- **Directors' personal cover**

  Directors who incur personal loss are covered as standard for all cover taken up by the main insured.

  How will it benefit? Directors' want to know their whole business is covered, including their own cyber losses, not just the company itself e.g. directors' transferring personal funds to a hacker or having their family photos held to ransom on their family photos held to ransom on their personal laptop.

- **Full GDPR coverage**

  Full GDPR coverage for data breaches, but also alleged breaches of the regulation.

  How will it benefit? Not all regulatory actions commence due to a data breach, there could be alleged breaches of GDPR which result in a regulatory investigation and this could be particularly pertinent for clients that hold significant amounts of personal data.

- **24/7/365 hotline**

  We will provide a 24 / 7 / 365 response line that the client can call anytime of day / week / year.

  How will it benefit? Would the MD / CEO know who to contact if something like this happens? Given the data held on individuals, they also need to be mindful of the 72 hour reporting requirements under GDPR. Would they know how to do this and investigate the breach within 72 hours and draft an appropriate response to the regulator without assistance?

- **CyberClear Academy**

  Access to a free cyber training platform if they go ahead which educates staff.

  How will it benefit? Insurers will reduce the excess by GBP 2,500 if 80% of networked employees complete the training which can be substantial for a small business. Completion of this training can also be used as evidence that the client has understood and thought about data security risks in the event there is a breach.

Ascend Broking Group Ltd
21 Springfield Lyons Approach, Chelmsford Business Park, Chelmsford, Essex CM2 5LB
Tel 01245 449 060 | Email info@ascendbroking.co.uk | Web www.ascendbroking.co.uk

YOUR BUSINESS IS AT RISK IF...

- you hold customer or employee data such as names, addresses, bank details, passport copies etc;
- you use a computer to operate;
- you have a website;
- you take payment via card;
- you store data in the cloud or rely on cloud-based services;
- you make electronic payments.

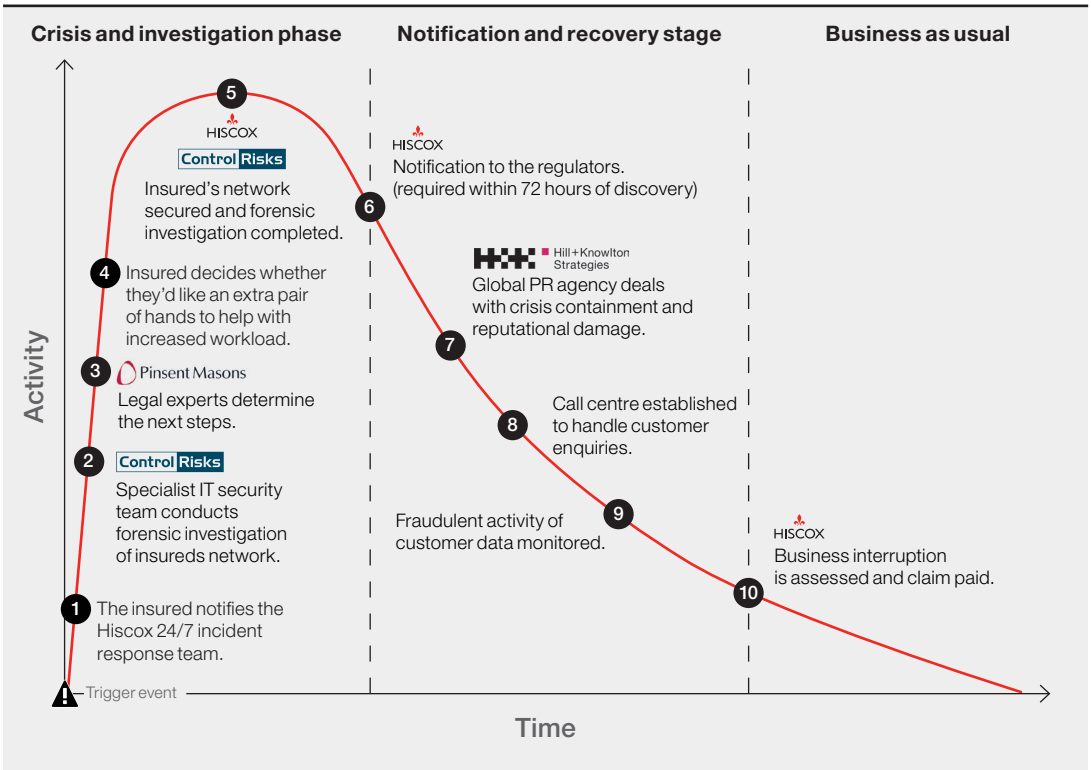
HOW YOU CAN PROTECT YOUR BUSINESS

Hiscox CyberClear has been developed to offer comprehensive, but flexible, cyber cover to UK businesses of any size – from one – person operations to multinationals – and can include protection against:

- data breaches – where personal or commercial information (electronic or otherwise) is accessed without authorisation;
- security failure – a hacker exploits weaknesses in your security systems, leaving your business exposed;
- cyber attacks – any digital attack against your business;
- extortion – criminals holding your systems or data to ransom or threatening to publish information;
- human errors – mistakes made by staff or suppliers that results in a data breach or system outage;
- business interruption – covering the loss of income that you may suffer from a cyber attack;
- GDPR – covering your liabilities and the cost of defending regulatory investigations after any alleged breach of data protection legislation;
- reputational damage – includes PR and crisis management support, and covers lost revenue or customers;
- financial crime and fraud – the use of the internet to deceive employees, customers or suppliers into transferring money or goods;
- property damage – physical damage to equipment or property resulting from a cyber attack;
- dependent business interruption – covering lost revenue or increased costs incurred if a supplier's systems are taken offline by a cyber incident.

[1] 45% of all of all businesses were hit by at least one cyber attack: Hiscox Cyber Readiness Report 2018.

HOW HISCOX CYBERCLEAR RESPONDS IN AN ATTACK



Key

Control Risks

Control Risks' cyber response team provides crisis management advisory support, technical forensics expertise and investigations capability to guide and support organisations through high-impact cyber incidents.

Pinsent Masons

Pinsent Masons' specialist cyber team will coordinate and project manage cyber events by supporting Hiscox insureds and working closely with our panel of third-party experts such as Control Risks/Hill+Knowlton to minimise the impact of the incident.

Hill+Knowlton Strategies

With over 85 offices in more than 45 countries and nearly 90 years' experience, Hill and Knowlton's world-class teams of trusted advisors and creative experts collaborate across time zones, languages and cultures to help clients make informed decisions and help strengthen brands, reputations and bottom lines.

HISCOX CYBERCLEAR VS. COMPETITOR COVER

	HISCOX CYBERCLEAR	AIG	Ascent Underwriting	Aviva	CFC Underwriting	Chubb	NIG	Optimum SR	Pen Underwriting	QBE	RSA	Travelers
First party	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Third party	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Business interruption	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Cyber terrorism	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Increased costs	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Crime	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Non-specific viruses	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Breach by supplier	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Employee data	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Transmission of virus	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Call centre costs	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Destruction of tangible property	✓	✓	✓	✓	✗	✗	✓	✗	✗	✗	✗	✓
Reputational harm	✓	✗	✗	✓	✓	✓	✗	✗	✓	✓	✗	✓
No aggregate or global limits	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗
Recreation of data if can't be restored	✓	✓	✓	✗	✓	✓	✓	✗	✓	✓	✓	✓

Insurance Times
Cyber Product Report
2018
HISCOX: BEST IN PRODUCT CLASS OCT 2018

WHY CHOOSE HISCOX CYBERCLEAR?

Hiscox CyberClear will help to protect your business from the financial and reputational costs of a cyber incident. If the worst should happen, you know that you will have the reassurance, support and advice from the UK's market-leading cyber insurer.

Access to the best experts in the business

Through Hiscox CyberClear you have instant access to a network of market-leading expertise from IT forensics to privacy lawyers and reputational experts.

Future proofed

Not only will Hiscox CyberClear cover you for today's risks, our extensive policy wording means that you're protected from emerging risks, threats and digital attacks that criminals may adopt in the coming years.

Breadth of cover

Hiscox CyberClear covers the financial cost and business impact of an incident, as well as offering a range of additional features; from worldwide cover as standard, key person cover and no overall policy aggregate limit, to a 72-hour excess waiver, directors' personal cover and no retroactive date.

Simple to understand

Hiscox CyberClear is just that… clear. There are no complicated modules. You know what you are buying and what you are covered for.

We know what we're doing

Hiscox has been providing this type of insurance since 1999, and has handled thousands of claims in that time. We know the risks your business faces – whether you're a two–partner legal firm or a tech business with hundreds of employees – and how best to manage and mitigate them.

VALUE ADDED SERVICES

Hiscox CyberClear Academy

Prevent a cyber incident happening through access to our online suite of cyber security training modules for you and your employees. Access to the academy is free to all Hiscox CyberClear customers with a revenue of less than £10 million.

HISCOX CYBERCLEAR® ACADEMY

Calculate the cost of a cyber attack

Hiscox and Deloitte have jointly developed the cyber exposure calculator to estimate the financial impact of cyber crime in worst-case scenarios, meaning you can manage your exposure.

#1

Hiscox CyberClear has been ranked the most comprehensive policy by the Insurance Times.[2]

[2] Insurance Times Best in Class Product – Oct 2018.

HISCOX CYBERCLEAR IN ACTION

Sector: Financial services
Turnover: £40m +
Claim cost: £226,000

A costly phishing trip

An employee at a financial services agency fell victim to a phishing incident in which a spoof email from one of the company's senior managers requested that the employee transferred £226,000 to a specified bank account. Believing the request to be genuine, the employee issued the fraudulent wire and both the agency's bank and the receiving bank were unable to recover the funds. The email was actually from a Gmail account created to imitate the senior manager's genuine address.

Hiscox response

On realising what had happened, the agency called us and we immediately engaged a data breach coach and IT forensics to confirm whether there had been any breach of the insured's systems or whether personal data had been compromised.

We reimbursed the money lost within a month of notification while it was confirmed that no breach of data had occurred so there was no need for any notification. Losses for payment diversion fraud can be offered as an additional cover to the standard Hiscox CyberClear policy.

Sector: Technology
Turnover: £40m +
Claim cost: £70,000

An IT firm falls victim

A technology company noticed that a piece of malware had been installed on one of its servers.

Hiscox response

We immediately instructed an IT forensics firm to investigate what the malware was doing and how it had been installed on our insured's systems. The server contained a substantial amount of personal data and so we also investigated whether there was any wider breach or risk that personal data had been compromised.

Given the potential gravity of the breach, we also instructed a breach coach to manage the investigation. The investigation confirmed that the malware was mining, but fortunately nothing more than this and there had been no wider breach.

Sector: Marketing
Turnover: Up to £1m
Claim cost: £39,000

Advertising for Bitcoin

A PR company noticed a problem with its emails. Its regular IT contractor investigated and concluded the most likely cause was malicious activity. The insured contacted us and we deployed an IT forensics team who were quickly on site to investigate and confirmed the insured had indeed been the victim of an attack.

The PR company's IT systems had been infected with cryptojacking malware to mine for cryptocurrency. They also confirmed that the hackers who deployed the malware had accessed the insured's systems and that personal data was potentially compromised.

Hiscox response

After investigating the extent of the breach, the IT team removed the malware and plugged the gap in the PR company's security which had allowed the breach. We then engaged legal counsel to advise the insured on its notification obligations, and then arranged the notification of the regulator and relevant data subjects.

Sector: Food services
Turnover: Up to £10m
Claim cost: £15,000

A large restaurant bill

A ransomware attack encrypted a restaurant's entire server, impacting its point of sale registers and meaning it was effectively unable to trade.

Hiscox response

Having exhausted all other options, it was clear that the most effective way to restore the restaurant's systems was to pay the ransom.

We covered the cost of the ransom, together with the associated IT costs of applying the decryption key and ensuring that the insured's business was back up and running. We also engaged a breach coach to confirm whether any personal data had been compromised. In addition to these costs, we covered the business interruption suffered by the restaurant as a result of being unable to trade.

[3] Insurance Times Cyber Product Report 2018.

HISCOX CYBERCLEAR: YOUR QUESTIONS ANSWERED

Why should I buy insurance for cyber risks?

You're most likely covered for risks like fire, flood and professional negligence but you are just as likely to suffer a cyber attack which can lead to loss of business, revenue and reputation; significant extra costs involved in dealing with the attack; and, regulatory penalties.

Doesn't my business insurance cover this risk?

No. Your standard business insurances will not provide the comprehensive protection you need against a cyber attack.

Hackers aren't interested in me, are they?

Much of the criminal activity online isn't specifically targeted at a particular business; those behind the attacks will often use tools to search the internet for any system that has a vulnerability. They will then exploit that vulnerability, regardless of who is sitting behind it.

I'm not an online business, so is this cover relevant for me?

A lot of companies identify as 'offline' and assume they don't need cyber insurance. However, virtually all UK businesses (98%) represented in a government survey[3] rely on some form of digital communication or services, such as staff email addresses, websites, online banking and the ability for customers to shop online, which exposes them to cyber security risks.

What does Hiscox CyberClear offer that other cyber insurance policies don't?

Hiscox CyberClear offers the broadest cyber cover available in the market, accompanied by a team of experts who will get your business back up and running fast in the event of an attack.

Does the policy only protect against hacking attacks?

No. Whilst cyber criminals are one of the biggest sources of claims, issues can also occur from human error, such as sending an email to the wrong address, leaving a briefcase on a train, or mistakes in configuring a system.

I don't hold any customer personal data – do I still need this cover?

The definition of personal data under GDPR is very broad, and would still include things like a business email address. You also need to consider suppliers' details, as well as information relating to employees (past, present and prospective). Additionally, the majority of claims that we deal with do not involve a breach of personal data, but loss of funds, data corruption, or system downtime – all of which you may be vulnerable to even if you do not hold much personal data.

For more information please contact your insurance broker.

[3] Government Cyber Security breaches survey 2018.

KNOWLEDGE IS POWER

Arm your clients with the Hiscox CyberClear Academy to protect themselves against a cyber attack.

The Hiscox CyberClear Academy is an online cyber security training platform designed to raise cyber security awareness among employees and help protect businesses from cyber threats.

Key features

- Training contains nine learning modules allowing employees to understand all aspects of cyber risk, including social engineering, online safety and information handling.
- The content is concise, relevant and is provided at regular intervals, saving time for employees whilst reinforcing key messages.
- The continual nature of the training helps to combat complacency and ensures that employees are equipped to deal with this ever-changing threat.
- Every module finishes with a short test to confirm that the content has been clearly understood. The progress of all employees can be monitored by your client's own appointed system administrator.

Stay cyber compliant

The Hiscox CyberClear Academy provides cyber awareness training for employees to help meet the requirements of regulators across Europe. Under the General Data Protection Regulation, organisations must implement 'appropriate technical and organisational measures' to protect the data they hold and process. Employee cyber awareness training constitutes a key operational measure.

Policy incentive

If 80% of clients' employees successfully complete the learning pathways, the excess shown in the schedule is reduced by £2,500. If the excess shown in the schedule is £2,500 or lower, no excess is payable.

Access

Access will automatically be granted to all Hiscox CyberClear policyholders with a revenue of below £10,000,000. Instructions on how to register for the first time will be included in their policy documentation.

If you would like to find out more about the Hiscox CyberClear Academy, please contact your local underwriter.

HISCOX
CYBERCLEAR® ACADEMY

Hiscox
1 Great St Helen's
London EC3A 6HX
United Kingdom

T +44 (0)20 7448 6000
E enquiry@hiscox.com
www.hiscoxgroup.com

18747 03/18

Ascend Broking Group

Business Insurance Solutions

Would you like to know more?

www.ascendbroking.co.uk/cyber-data-insurance

Ascend Broking Group Ltd 21 Springfield Lyons Approach, Springfield Lyons, Chelmsford, Essex, CM2 5LB

Tel 01245 449060 | Email info@ascendbroking.co.uk | www.ascendbroking.co.uk