Market Leading Cover

Ascend Broking Group
Business Insurance Solutions

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.

Benefit: Clients will have the comfort of knowing that their cyber policy is future proofed and will not only respond to attacks known in the current times, but also attacks 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 .

In partnership with the Police

With our policies, you will have access to a great new service, Police CyberAlarm. This is a free tool developed with the met police to help businesses understand and monitor malicious cyber activity.

Police CyberAlarm acts as a “CCTV camera” monitoring the traffic seen by a member’s connection to the internet. It will detect and provide regular reports of suspected malicious activity, enabling organisations to minimise their vulnerabilities.

Full GDPR coverage

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

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.

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.

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.

Your business is at risk if..

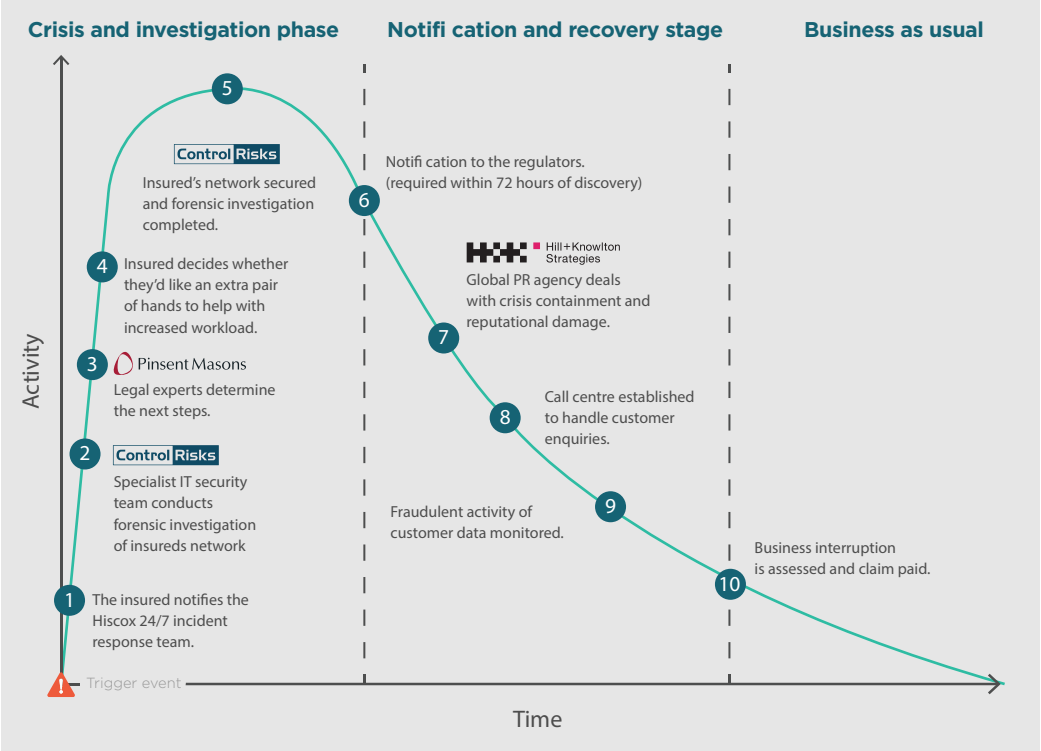
- you hold customer or employee data such as names, addresses, bank details, passport copies etc;
- you use a computer to operate;
- you have a website;
- you take payment via card;
- you store data in the cloud or rely on cloud-based services;
- you make electronic payments.

How you can protect your business?

Cyber covered 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 offl ine by a cyber incident.

How Cyber Covered responds in the event of an attack



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 offi ces 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.

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 Cyber-Clear customers with a revenue of less than £10 million.

HISCOX CYBERCLEAR® ACADEMY

Our Accreditation partners

With your Cyber Covered policy, you will receive a discount from our partners on cyber training, certification and accreditation.

CYBER ESSENTIALS

KYND Vulnerability reporting tool

To help the business understand their cyber risks from a technical perspective. Your policy will give you access to a full report on the business and highlight the key exposures for the business*.

KYND

An additional admin fee may apply for the report depending on business size.

Real Claims Examples

A selection of real claims and the remedial work carried out

Financial Services
Turnover: £5m
Claim cost: £116,000

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 £110,000 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.

Cyber Covered response

On realising what had happened, the Insured 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.

Technology
Turnover: £560k
Claim cost: £26,000

A tech startup in central London falls victim

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

Cyber Covered response

We immediately instructed an IT forensics firm to investigate what the malware was doing and how it had been installed on the insureds systems. The server contained a substantial amount of personal data 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.

Online Retailer
Turnover: £150k
Claim cost: £15,000

A malicious Service charge invoice

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

Cyber Covered response

Having exhausted all other options, it was clear that the most effective way to restore the insureds 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 insured as a result of being unable to trade.

Why choose Cyber Covered?

Cyber covered 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 Cyber Covered 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.

Cyber & Data Insurance

Your questions answered

Why should I purchase 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 existing 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 survey3 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 cyber covered offer that other cyber insurance policies don't?

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.

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.