HISCOX

CYBERCLEAR®

Cyber and data insurance

Policy summary

Your cover in a nutshell:

Hiscox CyberClear cyber and data insurance is designed to support and protect you from evolving cyber threats and risks associated with data, whether electronic or non-electronic. We will pay for claims and investigations made against you during the period of insurance arising from your cyber or data liability, up to the limit of indemnity in the schedule, and including your legal defence costs for covered claims and investigations.

We also pay for your own losses arising from cyber or data incidents discovered during the period of insurance, up to the limit of indemnity shown in the schedule.

We work with experts who offer practical support and assistance in the event of a claim, including specialist IT forensics, legal and PR firms.

Each of the covers is subject to an aggregate limit of indemnity, which is the most we will pay under that cover regardless of the number of claims, losses or investigations. In some cases, the Your own losses and Claims and investigations against you covers are subject to a combined aggregate limit. Your schedule will show if this is the case. The policy may also be subject to further limits for certain items, details of which are stated in the schedule.

You must pay the excess shown in the schedule for each claim or loss. For interruptions to your or a dependent business, or for increased costs of working arising from damage to your reputation, the excess is expressed as time excess, which is the period of time after the incident for which you are not covered.

Key benefits: what risks are you protected against?

Please check your policy schedule to see which of the following sections you benefit from.

1. Your own losses

We will pay for losses incurred by you if you suffer:

- the unauthorised acquisition, access, use or disclosure of personal data or confidential corporate information;
- a failure by you, or others on your behalf, to secure your computer system against unauthorised access or use;
- a threat to damage your systems or disseminate sensitive information, following unauthorised access to your systems;
- a digital attack designed to disrupt access to or the operation of your computer system;
- an interruption to your business caused by an act or omission of an employee or supplier in the handling of a data asset or the maintenance or development of your computer system; or
- an interruption to your business caused by a dependent business suffering a cyber attack.

If you suffer any of the above, we will pay:

- the costs of computer forensic analysis to confirm a data breach;
- legal costs incurred to manage a data breach;
- costs incurred in notifying data subjects and any regulatory body, and providing credit monitoring services;
- the cost of a ransom demand and specialists to handle ransom negotiations;
- additional business expenses caused directly by a cyber attack;
- costs to regain access to or restore your data assets from back-ups or other sources;
- your loss of income and additional costs of working if your business suffers an interruption or if your reputation is damaged;
- the costs to appoint a public relations consultant to protect your reputation and manage your media; and
- the costs to engage a consultant to manage your response to the incident.

We will also pay for the above where you have incurred loss as the result of a breach by a supplier of yours.

2. Claims against you

We will cover you if:

- a claim is made against you for breach of confidence, personal data, sensitive commercial information or any contractual duty of confidentiality;
- an investigation is commenced arising from the unauthorised acquisition, access, use or disclosure of data, or breach of a law governing the handling of personal data, including GDPR investigations;
- a claim is brought against you for breach of PCI-DSS;

HISCOX

CYBERCLEAR®

- a claim is brought against you for infringement of intellectual property rights, defamation or breach of licence arising from your email, website or social media accounts; or
- a claim is brought against you for transmission of a virus, denial of service attack or prevention of authorised access to a computer system or data.

3. Financial crime and fraud

We will pay for your losses if you discover a loss from:

- electronic theft of money, securities or property;
- criminal use of your telephone lines;
- you transferring money, securities or property in direct response to a social engineering communication;
- a client transferring money, securities or property in response to a social engineering communication following a breach of your network;
- the fraudulent or dishonest use of your electronic identity.

4. Property damage

If any insured equipment shown on the schedule is rendered unusable as a result of a security failure, cyber attack, hacker or transmission of a virus, we will pay the costs of repairing or replacing the unusable part of the equipment.

5. Additional covers

We will also:

- pay to upgrade existing hardware and software and to obtain risk management advice to prevent or minimise a recurrence of certain claims or losses;
- cover your statutory directors, partners or officers if they suffer a loss or a claim is brought against them in their personal capacity which would have been covered under the policy if suffered by, or brought against, you; and
- pay court attendance compensation.

Significant or unusual exclusions and limitations:

We do not pay for any claims, losses, breaches, privacy investigations or threats due to:

- the provision of professional advice or services;
- the failure of service provided by an internet service, telecommunications or utilities supplier, or any other infrastructure provider;
- breach of intellectual property rights, other than where arising due to a data breach by a third party, a security failure, or any claim under the Online liability section;
- a hack by a partner or director of yours;
- personal injury or damage to tangible property, other than where covered under the Property damage section;
- degradation or deterioration of your computer system, other than due to operational error;
- the use of any outdated or unsupported software or systems;
- anything you knew or ought reasonably to have known about before the policy started;
- any acts or omissions you deliberately or recklessly commit, condone or ignore;
- any post from a social media account that does not belong to your business;
- online liability claims brought by your current or former employees; or
- any criminal, civil or regulatory fines, other than PCI charges and regulatory awards where legally insurable.

We will also not make payment:

- unless you notify us promptly of anything which is likely to give rise to a claim under this section; or
- for cyber extortion unless you inform or allow us to inform the appropriate law enforcement authorities.

We may reduce any payment we make equal to the detriment we have suffered if you:

- do not take all reasonable steps to negotiate with the supplier of any services to reduce or waive any charges that were not legitimately incurred for the purposes of your business; or
- admit that you are liable or make any offer without our prior written agreement.

If you notify us within 72 hours of your first awareness of any actual or suspected data breach, we will waive the excess in respect of that breach. This does not apply to any time excess.