HISCOX

CYBERCLEAR®

Cyber and data insurance

Policy summary

Policy wording ref: 19029 WD-PIP-UK-CCLEAR(5)

Key benefits: what risks are you protected against?

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. The policy may also be subject to further limits for certain items, details of which are stated in the schedule.

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.

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;
- 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. Cyber business interruption

if you suffer:

- an interruption to your business caused by a covered breach, cyber attack, illegal threat or security failure;
- 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.

we will pay:

- your loss of income and additional costs of working if your business suffers an interruption or if your reputation is damaged;
- alternatively to your loss of income and additional costs of working, where shown on your schedule, we will pay you a daily interruption benefit;
- 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.

3. Claims and investigations 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;
- a claim is brought against you for infringement of intellectual property rights, defamation or breach of licence arising from alterations or additions made by a hacker to 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.

4. Your losses from crime

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

- electronic or physical theft of money, securities or property;
- dishonesty or fraud carried out by your employee;
- 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.

5. Cyber 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.

6. 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:

- your breach of duty in the provision of products or services to your client, other than claims made directly against you by data subjects in respect of their own personal data;
- 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 any claim under the Online liability section;
- personal injury or damage to tangible property, other than where covered under Online liability, Your losses from crime or Cyber property damage;
- war or due to cyber operations carried out by, at the direction or under the control of a state;
- 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;
- the use of any credit, debit, access, convenience, smart, identification or other card, other than losses caused by the dishonesty of an employee who uses a card that you have issued to them for the payment of valid business expenses incurred for or on behalf of you;
- any purchase, use or development of blockchain or any other distributed ledger technology, however this does not apply to covered cyber ransom losses;
- any pollution;
- any criminal, civil or regulatory fines, other than PCI charges and regulatory awards where legally insurable; or
- any actual or alleged monitoring, tracking or profiling of an individual without their authorisation, including, but not limited to, web-tracking, session recording, digital fingerprinting, behavioural monitoring, eavesdropping, wiretapping or audio or video recording by you or by a third party.

Additionally, we do not pay your losses from crime due to:

- any act, breach or omission committed by any employee after you first discovered any crime being committed by or in collusion with that employee;
- any act, incident or event occurring, or any loss suffered before the crime retroactive date;

- the use of any actual or counterfeit letter of credit, bill of lading, shipping document, warehouse receipt, account receivable, or any other similar document unless the loss arises as a direct result of dishonesty of an employee or loss of assets.

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.

You must pay the excess shown in the schedule for each claim or loss. For loss of income, increased costs of working, or additional increased costs of working claims, the excess is expressed as time excess, which is the period of time after the incident for which you are not covered. No excess applies to claims for the daily interruption benefit, but such claims will only be paid where the interruption exceeds the waiting period.

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.