HISCOX

CYBERCLEAR®

Cyber and data insurance

Policy summary

Policy wording ref: 19029 WD-PIP-UK-CCLEAR(6)

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:-

- your own losses arising during the indemnity period from cyber or data incidents discovered during the period of insurance;
- claims and investigations made against you during the period of insurance arising from your cyber or data liability, including your legal defence costs for covered claims and investigations,

up to the limit of indemnity stated in the schedule, which also includes further limits which apply to particular covers.

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

A. 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 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.

We will also pay your additional business expenses caused directly by a cyber attack including the costs to regain access to or restore your data assets, together with the costs of a public relations consultant to protect your reputation and manage your response to the incident.

B. Cyber business interruption

if you suffer:

- an interruption to your business caused by a covered breach, cyber attack, illegal threat or security failure; and/or
- if you have purchased:
  - the operational error business interruption extension and suffer an interruption to your business caused by a non-malicious act or omission by an employee in the handling of a data asset or the maintenance or development of your computer system; and/or
  - the dependant business interruption extension and suffer an interruption to your business caused by a dependent business suffering a security failure or cyber attack,

we will pay:

- your loss of income, and increased costs of working resulting solely and directly from the interruption, together with your loss of income if any of your customers terminate or decide not to renew their contract(s) with due to the interruption to your business.
- in the alternative, if stated on your schedule, we will pay you a daily interruption benefit;

C. 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 or 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

HISCOX

CYBERCLEAR®

- a claim is brought against you for transmission of a virus, denial of service attack or prevention of authorised access to a computer system.

D. Your losses from crime

We will pay your losses arising directly from crime, which includes the electronic or physical theft of money, securities or property, dishonesty or fraud carried out by your employee, the fraudulent or dishonest use of your electronic identity or you transferring money, securities or property in response to a social engineering communication.

E. Bricking

If any property which you own, and which through digital connectivity is connected to your computer system used for your business 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.

F. 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 a reward at our discretion for information leading to the arrest and conviction of those responsible for causing the loss.

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 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 bricking;
- 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 computer system;
- any purchase, use or development of blockchain or any other distributed ledger technology, however this does not apply to covered cyber ransom losses;
- any actual or alleged monitoring, tracking or profiling of an individual without their authorisation;
- any failure to comply with a federal, state or local law of the United States of America or Canada relating to the use, collection, processing or storage of biometric or genetic data;
- cyber extortion, unless you inform or allow us to inform the appropriate law enforcement authorities.

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;
- 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.

Please refer to your schedule and policy wording for further information regarding the applicable time excess or waiting period, which is the period of time after the incident for which you are not covered.

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, other than for cyber business interruption losses or in respect of your losses from crime.