HSB Cyber Insurance

HSB Distributor Product Information

Information for distributors of HSB insurance products only

HSB

A Munich Re company

This document has been produced by HSB in accordance with our regulatory responsibilities as a Product Manufacturer. This document provides high level information on the product, including information on the main features and exclusions, target market, fees, commissions, distribution channel, as well as Fair Value outcome and Consumer Duty regulations. It is intended for use by our Distributors and not for customers or operational staff. For more information, please speak to your HSB representative.

It is not a sales or marketing tool and should not be used as such.

Requests for insurance coverage should always be placed under the most suitable product based on the Insured's needs and in their best interests.

Carrier name:	HSB Engineering Insurance Limited
Broker name:	As stated in TOBA
Product name:	HSB Cyber Insurance
Reference/UMR (Binder):	POL-UKG-CYB-002-TRA POL-ROI-CYB-003-TRA
Reference (class of business):	Computer, data and cyber-risks.
Date:	March 2024

Product information

Product oversight and governance

HSB Engineering Insurance Limited has an established Product Approval Process that covers the entire product lifecycle, from new product development to product review. The following elements are included within the process:

- Extensive research of the product concept is undertaken to identify an appropriate target market.
- Customer type, distribution channel, charging structure as well as the wider market and legal developments are identified and considered.
- Risk assessments and regulatory reviews are undertaken to ensure fairness to customers and that any risks to the identified target market are appropriately managed.
- Product marketing, training and technical support ensures knowledge of the product is accurately assessed and competence is evidenced prior to distribution of the product.
- Post launch, the overall product performance is interrogated and reviewed. This includes claims reports, systems reviews and customer feedback being processed to identify on-going product and market suitability.

Product summary

A commercial product designed to provide cover for computer, data and cyber risks which could be damaging to a business and its reputation. Issues can range from data recovery following a hardware failure to a full scale data-breach. The product provides access to a network of cyber risk experts who can help to minimise the disruption to a business. The product provides cover for :

- Hardware - loss, damage, theft, breakdown and corruption of hardware (including portables and electronic office equipment);
- Data corruption and extra cost - reconfiguration and data restoration costs following damage to hardware, prevention of access or a cyber event;
- Cyber crime - financial loss resulting from fraudulent access of your computer system and (if the carrier agrees) payment of ransom demands following threat of damage to your computer system by virus, hacking or data disclosure;
- Cyber liability – damages and defence costs arising from a claim made against the customer following failure to secure data, unintentional virus transmission or loss of reputation resulting from the content of a website or data processed by the customer's computer system;
- Data-breach expense – the cost of a customer's failure to keep to their data privacy obligations e.g. breach identification, notification to affected parties etc;

- Cyber event – loss of business income – loss of income following a cyber event or prevention of access.

All six sections of cover are available to the customer however in order to have the cover provided by section 2 (Data corruption and extra cost), section 3 (Cyber crime), section 4 (Cyber liability), section 5 (Data-breach expense) or section 6 (Cyber event – loss of business income), the customer must have first selected cover under section 1 (Hardware). The policy offers flexibility so that different levels of cover can be selected within the six sections.

HSB Cyber Insurance provides our customers with a market option of comprehensive cyber risks cover in one standalone product.

Other information

- **Territorial limits** – the product is available only to customers domiciled in the UK and Republic of Ireland (ROI).
- **Policy renewal** – policy renewal is not automatic but renewal is normally invited (by the carrier via the distributor) as a policy approaches the end of the current period of cover.
- **Claims notification** – all claims are notified to the carrier whose claims team manages the lifecycle of each claim in line with corporate claims handling procedures.
- **Complaints notification** – all complaints are notified to the carrier whose complaints team manages the lifecycle of each complaint in line with corporate complaints handling procedures.
- **Carrier fees** – None.

Target market

The HSB Cyber Insurance policy is a commercial product designed to cater for the needs of commercial entities with electronic devices to process data for business purposes. The product is designed to protect the insured's computer systems and data against loss and damage covering events to protecting the insured from cyber risks which could be damaging to their business and reputation. Issues can range from data recovery following a hardware failure to a full scale data-breach. The product is aimed at but not limited to Small to Medium Enterprises (SMEs).

Types of customer for whom the product would be unsuitable

- Financial institutions / payment processors such as; banks, building societies, credit card companies, loan companies, card payment processors / clearing houses, investment companies, central post offices or any organisation providing finance/credit or bank accounts;
- Any trades involving gambling / gaming such as betting shops, online betting and lotteries;
- Publishing, broadcasting and media (news, books, radio, TV, advertising);
- Website and software designers / suppliers;
- The product is not suitable for consumers or retail customers.

Distribution Strategy

This product is designed to be delivered to customers via UK and ROI open market brokers. As well as traditional transactional distribution the product maybe distributed via approved exclusive broker arrangements and approved delegated authority arrangements.

Any notable exclusions or circumstances where the product will not respond

General

Restrictions

- There is a 'Cyber attack limit' which is the most the carrier will pay in total for the period of insurance for all losses resulting from a cyber attack.
- The customer (and any service provider) must back up original data at the frequency specified. Precautions must also be taken to make sure that all data is stored safely.
- The customer's computer system must be protected by a virus-protection software package and protected by a firewall on all external gateways to the internet.
- In respect of section 4 (Cyber liability) and section 5 (Data-breach expense) the customer must be registered with the relevant data protection authority and must ensure that appropriate procedures are in place to protect data.

Exclusions (what is not insured)

- Loss or damage resulting from infectious agents or pandemics.
- Loss or damage resulting from intentional acts.
- Losses caused by atmospheric or environmental conditions causing interference with satellite signals.

Section 1 – Hardware

Restrictions

Hardware must be maintained, inspected and tested as recommended by the manufacturer and a record of maintenance and data back-up procedures must be kept. Hardware must not continue to be used after damage

Exclusions (what is not insured)

Damage covered under any manufacturer's warranty or maintenance contract

Section 2 – Data corruption and extra cost

Restrictions

Hardware must be maintained, inspected and tested as recommended by the manufacturer and a record of maintenance and data back-up procedures must be kept. Hardware must not continue to be used after damage

Exclusions (what is not insured)

- Data-breach (although covered under section 5).
- The cost or loss caused by or resulting from an external network failure, unless resulting from physical damage to the network or other property.

Section 3 – Cyber crime

Exclusions (what is not insured)

- Financial loss resulting from fraudulent use of a credit or debit card.
- Fraudulent credit applications.
- Hacking by directors and officers or employees.

Section 4 – Cyber liability

Exclusions (what is not insured)

- Deliberate defamation or disparagement.
- Mistakes concerning your business in financial statements or representations.
- The customer breaking corporate laws or regulations.
- Infringement of patent.
- Employer liability, product liability or professional indemnity.

Section 5 – Data-breach expense

Exclusions (what is not insured)

Costs to restore the customer's computer systems and data (although covered under section 2).

Section 6 – Cyber event – loss of business income

Exclusions (what is not insured)

The cost or loss caused by or resulting from an external network failure, unless resulting from physical damage to the network or other property.

Other information which may be relevant to distributors

A ‘cyber event’ is defined as:

- loss, corruption, accidental or malicious deletion of or change to, unauthorised access to, or theft of data;
- damage to websites, intranet or extranet sites;
- damage or disruption caused by computer virus, hacking or denial of service attack; or
- failure of or variation in the supply of electricity or telecommunications networks owned and operated by you;
- affecting your computer system, the computer system of a service provider or customer of yours.

Cover under this product may be affected where:

- a fair presentation of the risk is not provided to the carrier;
- a delay in the notification of a claim prejudices the position of the carrier;
- the requirements of any condition precedent (an important term which sets out a step or action that the customer must take) are not met.

Consumer Duty and Fair Value

In accordance with the FCA PROD4 rules and consumer duty requirements, a product review and fair value assessment are completed annually for this product.

The requirements of these annual exercises consider good customer outcomes based upon the following areas:

- Product and services
- Price and value
- Consumer understanding
- Consumer support

For each of the four key areas, we have assessed what we understand the customer would consider a good outcome. These identified outcomes are:

Product and Services

- Customers are provided with a product that meets their needs
- Customers are provided with a product where the policy limits are appropriate and sufficient
- Customers are provided with a product where the policy coverage meets their expectations
- Customers are provided with clear and easy to understand policy and associated documentation

Price and Value

- Customers are provided with a product where the cost price is fair
- Customers are provided with a product where the distribution costs do not adversely affect the product's value

Consumer Understanding and Consumer Support

- Customers view marketing content that is clear, fair and not misleading
- Customers deal with intermediaries that are well informed and understand our product
- Customers that are vulnerable are identified and appropriate adjustments made
- Customers are provided with all the necessary information to make an informed decision
- Customers receive relevant documentation in a timely manner
- Customers individual needs are considered when they need to use their policy
- Customers can understand all of the terms and conditions of their policy and understand their obligation
- Customers are responded to a timely manner in an appropriate way
- Customers clearly understand how to make any adjustments to their policy and what happens next
- Customers clearly understand how to make a claim and what happens next
- Customers have easy access to making a claim and are well informed throughout the claims process
- Customers are satisfied how they are dealt with when making a claim
- Customers clearly understand how to make a complaint and what happens next
- Customers have easy access to making a complaint and are well informed throughout the complaint process

The review and assessment include insight from the monitoring of key reporting indicators surrounding but not limited to the following areas:

- Customer satisfaction surveys/market research
- Broker feedback
- Service delivery data
- Product reviews including testing of the customer journey
- Fair value assessments
- Retention rates
- Cancellation rates
- Complaints data
- Claim acceptance rates
- Declinature rates
- Frequency of claims
- Loss ratios
- Call handling data

Date of last fair value assessment:	Q1 2024
Outcome of last fair value assessment:	Fair Value

Comments

The product provides fair value to customers and is working as designed. Key metrics on usage and product value are monitored and there are no concerns that the product cannot be used or that there are any barriers to claim.

This product meets the needs within the Target Market Statement (as noted above)

The product has been subject to HSB Engineering Insurance Limited‘s full product review process and signed off by our authorised approvers as representing fair value to customers and may continue to be marketed and distributed.

Expected date of next fair value assessment	Q1 2025

DPI-GEN-CYB-002-TRA-1.00