HSB CyberPro

Insurance Product Information Document

Company: HSB Engineering Insurance Limited

Registered in England and Wales: 02396114, Chancery Place, 50 Brown Street, Manchester M2 2JT. Registered as a third country branch in Ireland: 906020, The Reflector, East Wing, 8 Hanover Quay, Dublin 2, D02 R573. HSB Engineering Insurance Limited is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority in the United Kingdom, and is authorised and regulated by the Central Bank of Ireland as a third country branch in the Republic of Ireland.

Product: HSB CyberPro

This Insurance Production Information Document provides an overview of the main features of the HSB CyberPro Insurance policy, and does not go into detail about all of the terms and conditions. You should read the policy document for full details of cover and the policy schedule for the sums insured and any endorsements which will be specific to you.

What is this type of product?

The HSB CyberPro product is designed to provide assurance and protection against suspected or actual cyber incidents which can be both disruptive and damaging to your business. The product provides a 24/7 unlimited incident response service providing assurance and guidance following suspected cyber incidents such as phishing scams, the fraudulent accessing of your data, the introduction of a computer virus etc. Additionally the product provides insurance protection against cyber risks ranging from data recovery following hardware failure to the cost of dealing with a a full-scale data-breach.

What is insured?

Insurance is provided for all the sections of cover noted below. Cover is provided for each occurrence up to the sum insured shown in the policy schedule.

Section 1 - Cyber incident response service

✓ The cost of an incident response case manager to assist you in responding to (as follows) any suspected or actual cyber incident first discovered during the period of insurance.

- Technical assistance
- Incident containment
- Impact mitigation
- Ongoing support

Section 2 – Computer system damage

Following a cyber event (loss or corruption of data; damage to websites; damage caused by computer virus, hacking or denial of service attack; failure of or variation in the supply of your own electricity or telecommunications network; affecting your computer system, the computer system of a service provider or customer of yours):

✓ The cost of reconfiguring your computer system including the cost of restoring data (this includes the computer system of a service provider).

✓ The cost of locating and removing a virus from your computer system.

✓ Consultancy costs on virus and hacking prevention.

Section 3 – Loss of business income and extra costs

Following a cyber event:

✓ Loss of income and extra costs to reduce disruption to your computer system.

What is not insured?

Below you will find information that highlights the main exclusions within each section of the policy.

✗ In respect of section 2 (computer system damage) and section 3 (loss of business income and extra costs) the cost or loss caused by or resulting from an external network failure, unless resulting from physical damage to the network or other property.

✗ In respect of section 2 (computer system damage) the value of data to you even if it cannot be restored or recreated.

✗ In respect of section 4 (cyber crime) financial loss resulting from.

- fraudulent use of a credit or debit card; or
- fraudulent credit applications.

✗ In respect of section 6 (cyber liability) deliberate defamation or disparagement.

✗ Loss, damage or expense caused by or in consequence of war.

✗ 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.

✗ The excess and time excess. (not applicable to section 1)

Section 4 – Cyber crime

✓ Financial loss resulting from fraudulent use of data in your computer system.

✓ Payments due to your telephone service provider resulting from hacking.

✓ The cost of responding, and if we agree in writing, the payment of a ransom demand, if you are the victim of crime such as a threat of damage to your computer system by virus, hacking or disclosing your data.

Section 5 – Data-breach expense

Following the failure of your business to keep to its data privacy obligations:

✓ Consultancy costs to investigate the breach and provide guidance on how to respond.

✓ The costs of notification to affected parties and regulators.

✓ The cost of providing credit file monitoring, identity theft assistance and a helpline to all affected parties.

✓ Public relations costs to minimise reputational damage.

Section 6 – Cyber liability

✓ Damages and defence costs arising from a claim first made against you as a result of:

- you or your service provider failing to secure data;
- you unintentionally transmitting a virus; or
- loss of reputation resulting from the content of your website, emails, or data processed by your computer system.

Extra cover

✓ Accountants fees.

✓ Avoiding corruption.

✓ Fines and penalties.

✓ Investigation cost.

✓ Loss-prevention measures.

✓ Removing data.

✓ Security audit.

✓ Temporary and fast-tracked repair.

Are there any restrictions on cover?

If you do not comply with certain conditions of the policy it may be cancelled or we may not pay your claim. Below you will find details of restrictions that apply to the policy.

! If you (or anyone acting for you) make a claim that you know is in any way false or exaggerated, we will not pay the claim and we may cancel the policy.

! You must back up original data at least every seven days. You must ensure that any service provider backs up your data in line with this required period. You must take precautions to make sure that all data is stored safely.

! Your 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 5 (Data-breach expense) and section 6 (Cyber liability) you must ensure that appropriate procedures are in place to protect data.

Where am I covered?

✓ You are covered at any insured location, provided the insured entity is domiciled in the United Kingdom. Claims must be brought within the jurisdictions specified in the policy wording.

What are my obligations?

– Your responsibility to provide us with a fair presentation of the risk

You must do everything reasonably possible to make sure that the information you give us is a fair presentation of the risk and you must make sure that you tell us immediately about any changes that may affect your cover. This is important before you take out the policy as well as during the period of insurance. You should also regularly review the cover provided to make sure it meets your needs, if your circumstances change you must tell the person who arranged your insurance for you, or us.

– Speaking to us about a cyber incident

If you have identified or suspect a cyber incident (for example a phishing scam, fraudulent accessing of your data, the introduction of a computer virus etc.) then you should contact our Incident Response Team (24/7 helpline) as follows:

Tel: +44 (0)330 100 9362
(calls to this number are charged at the same standard landline rate as calls to 01 or 02 numbers)

E-mail: cyberincident@hsbeil.com

– Making, or speaking to us about, a claim

Usually claims will be notified on your behalf by our Incident Response Team (see above) and they will guide you through the process however should you want to make a claim yourself (or talk to us about an existing claim) then please contact us:

– by speaking to the person who arranged this insurance for you; or

– by using the same contact details as above; or

– at the address below.

Address: Claims Department,
HSB Engineering Insurance Limited
Chancery Place
50 Brown Street
Manchester M2 2JT

– Change in circumstances or alteration in risk

As soon as you (or anyone acting for you) become aware of any change in circumstance which may affect your policy, you must tell us as soon as possible and keep to any extra terms and conditions.

When and how do I pay?

You must pay the premium on or before the start date of the period of insurance, or on dates agreed by us, to the person who arranged this insurance for you. If you do not pay the premium on time, we may cancel the policy.

When does the cover start and end?

The length of time covered by the policy will be shown in the the schedule (usually for a period of 12 months). This policy does not renew automatically.

How do I cancel the contract?

You have 14 days to make sure that you are happy with the cover provided – this 14 day period is known as the 'cooling-off period'. You can cancel the policy by telling the person who arranged this insurance for you or by telling us in writing and returning the schedule.

If you do cancel the policy within the cooling-off period, as long as you have not made a claim, we will refund all the premium you have paid. If you have made a claim, you will not get a refund.

You can cancel your policy at any time after the cooling-off period by telling the person who arranged this insurance for you, or by telling us in writing, and returning the schedule. If you have made a claim, you will not get a refund. If you have not made a claim, when we receive your notice and schedule, we will cancel the policy and send you a pro rata refund.