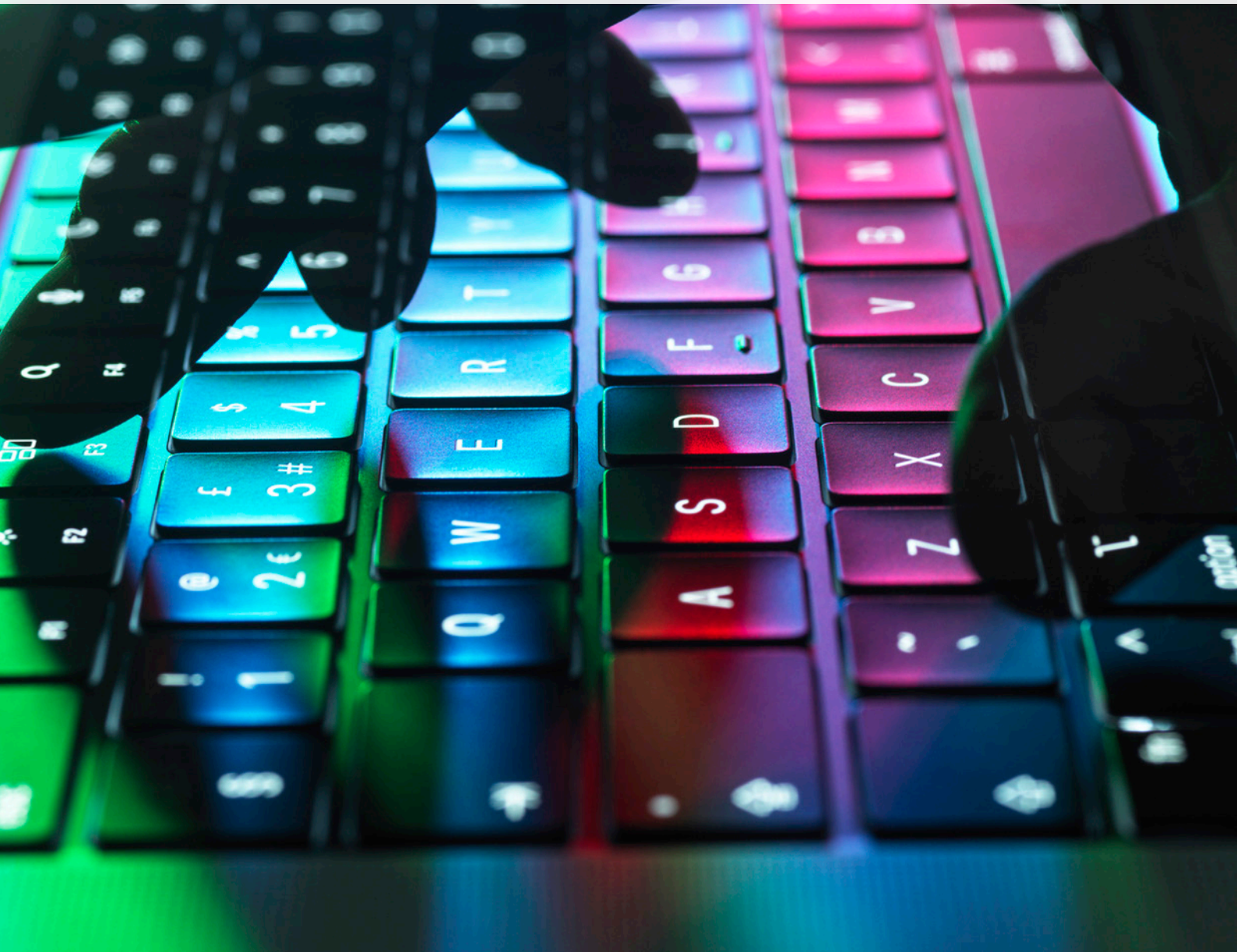
HSB

A Munich Re company

Policy Document

HSB CyberPro

Cyber incident response and insurance for UK businesses



What you should do if you discover 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:

Telephone: +44 (0)330 100 9362

(calls to this number are charged at the same standard landline rate as calls to 01 or 02 numbers)

Alternatively, if you prefer you can contact us at the following email address.

Email: cyberincident@hsbeil.com

This helpline is available to you **24/7** (**363 days a year***) throughout the period of insurance and can be used free of charge on an unlimited basis. There is **no policy excess charge for this service**.

If our Incident Response Team are unable to resolve your issue, then they will inform you as to whether you may be able to claim against your policy for any losses or additional expense resulting from your cyber incident. At this point our Incident Response Team will hand you over, and provide all details of the incident, to our Claims Management Team.

Then our Claims Management Team will become your point of contact (same contact details as above) through to the conclusion of your claim. Please note at this point there may be a policy excess to be deducted from any claim settlement.

**not available 25th December and 1st January*

Contents

Your contract with us 3

Important information 4

Headings and interpretation
Your policy
Your responsibility to provide us with a fair presentation of the risk
Your rights to cancel your policy
Our rights to cancel your policy
Our regulators
What happens if we cannot meet our liabilities
How we use your information
The laws and jurisdiction that apply to your policy

Contacting us 6

Speaking to us about a Cyber incident
Making, or speaking to us about, a claim
Making a complaint
Making any other enquiry

Definitions 7

What we will pay for 9

1 - Cyber incident response services
2 - Computer system damage
3 - Loss of business income and extra costs
4 - Cyber crime
5 - Data-breach expense
6 - Cyber liability

Extra cover 11

How much we will pay 12

Claim conditions 13

General conditions 14

What we will not pay for 15

Your contract with us

Thank you for buying the cyber insurance policy from us, HSB Engineering Insurance Limited (HSBEIL). We are pleased that you have chosen our policy, and we will work hard to make sure that you are happy with the cover and service you receive.

The policy is a legal contract between:

– you, the person or organisation shown in the schedule as 'The insured'; and

– us.

The policy is made up of this document, the schedule setting out details of your cover, and any endorsements shown in the schedule. These make up the entire contract between you and us and must be read together. Please keep them all safely together.

We used the information you gave us on your proposal, and any further information we received, to decide whether to insure you. If any of that information was not accurate or was incomplete, this could affect your cover (see 'Your responsibility to provide us with a fair presentation of the risk' under 'Important information').

If you pay the premium shown in the schedule, and keep to the terms and conditions of the policy, you will be covered under the sections of this document shown in the schedule for the **period of insurance**.

This policy has been issued by HSB Engineering Insurance Limited

Important information

Headings and interpretation

Throughout this policy:

- words or phrases which appear in bold have the meanings shown in the 'Definitions' section;
- headings are only to help you find the information you need, they do not form part of the policy wording;
- words which appear in the singular include the plural and vice versa;
- words which appear in the present tense include the past tense and vice versa; and
- any words after the terms 'including', 'include', 'in particular', 'for example' or any similar expressions are examples and will not limit the meaning of the words.

Your policy

This document, together with the schedule and any endorsements shown in the schedule, contains the information you need to know about your insurance. This document contains important information such as the terms and conditions of your insurance and how to contact us. The schedule and endorsements show:

- which sections of this document apply;
- the **sum insured** (the maximum amount of cover you have); and
- the premium.

Please keep the schedule with this document. We will send you a new schedule whenever there is a change to your insurance. We will also send you renewal documents each year before the renewal date shown, so you can check that the cover still meets your needs.

Your policy provides cover against specified events. Read this policy carefully to make sure that it meets your needs and you understand what is and is not covered. If there is anything you need to change or do not understand, contact the person who arranged this insurance for you, or you can contact us. You can find the contact details for your local HSBEIL office on our website at www.hsbeil.com.

Additional customer support

Should you require your policy documentation in an alternative format please contact the person who arranged this insurance for you, or you can contact us. You can find the contact details for your local HSBEIL office on our website at www.hsbeil.com.

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

You, or anyone acting for you , must make a fair presentation of your risk to us, not only when you first buy your policy, but also at each renewal and/or if you ask us to make any mid-term change to the policy during the **period of insurance**.

This means that the information you give us in your proposal is complete and accurate so has not been misrepresented in any way, and that you have made a fair presentation of the risk to be insured by disclosing every material fact and circumstance which you know or ought to know. A fact or circumstance is material if it would influence the judgment of the underwriter when considering whether to accept the risk and on what terms, conditions and premium. If you are in any way unsure whether or not a fact or circumstance is material to disclose, please consult the person who arranged this insurance for you or contact us.

If you fail to make a fair presentation and if:

- your failure is deliberate or reckless, we will treat your policy as if it never existed, refuse all claims and keep any premium you have paid. If your failure occurs during a change to your policy we will terminate your policy from the date of that change, refuse subsequent claims and keep any premium you have paid.
- your failure is not deliberate or reckless and we would not have issued your policy had you made a fair presentation, we will treat your policy as if it never existed and return any premium you have paid. If your failure occurs during a change to your policy we will treat your policy as though the change was not made and return any extra premium you paid.
- your failure is not deliberate or reckless and we would have issued or changed your policy on different terms had you made a fair presentation, we will;
  - alter the terms of your policy to those we would have imposed (other than those relating to premium); and/or
  - reduce the amount paid or payable on any claim in proportion to the amount of any additional premium that we would have charged.

As set out in general condition 1 – 'Alteration in risk', you, or anyone acting for you, must tell us about any change in circumstance which happens either before or during the **period of insurance** which may affect your cover (for example, something that increases the risk or something we asked you about when we accepted your proposal).

Important information

Your rights to cancel your policy

Cooling-off period
You have 14 days to make sure that you are happy with the cover provided. 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. This 14-day period, known as the 'cooling-off period', starts on:

– the day you receive your policy; or

– the date the **period of insurance** starts;

whichever is later.

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.

If the **period of insurance** is less than the cooling-off period then the rights detailed above are not applicable.

After the cooling-off period
You can cancel your policy at any time during the **period of insurance** 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 refund. That refund will be a percentage of the year's premium, based on the number of days left in the **period of insurance**, less a cancellation charge (10% of the year's premium). If the amount of premium you have actually paid does not cover the period you have been insured for, you must pay us the difference.

Our rights to cancel your policy

We may cancel your policy if you do not keep to:

– general condition 6 – 'Paying the premium'; or

– general condition 8 – 'Reasonable care'.

If we cancel your policy because you have not kept to the conditions shown above, we will send at least 14 days' written notice to the last known address we have for you. If you have not made a claim, we will refund a percentage of the premium based on the number of days left in the **period of insurance**. If you have made a claim you will not get a refund and you must pay us any amount you still owe for the period during which you have been insured.

Our regulators

HSB Engineering Insurance Limited is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.

The Financial Conduct Authority's website includes a register of all regulated firms.

You can contact the Financial Conduct Authority at:

Financial Conduct Authority
12 Endeavour Square
London E20 1JN
Telephone: 0800 111 6768
Website: www.fca.org.uk

What happens if we cannot meet our liabilities

If we cannot pay you what we owe, you may be entitled to compensation under the Financial Services Compensation Scheme (FSCS).

You can get more information about the scheme by contacting the FSCS at:

Financial Services Compensation Scheme
PO Box 300
Mitcheldean GL17 1DY
Telephone: 0800 678 1100
Website: www.fscs.org.uk

How we use your information

We are the controller of any personal information (for example, names, addresses, telephone numbers, job titles or dates of birth) you provide to us, or which is processed in connection with your policy. We collect and process information about you that we consider to be necessary in order to make decisions about the cover we provide to you, any claims you make, or to detect and prevent fraud. We also may record incoming and outgoing telephone calls with you for training, monitoring and quality control purposes.

We may share your information with, and obtain information about you from, companies within the Munich Re Group, other insurers, brokers, loss adjusters, credit reference agencies, fraud prevention agencies or other third parties who provide services on our behalf.

For further details on how your information is used and your rights in relation to your information, please see our Privacy statement at www.hsbeil.com.

The laws and jurisdiction that apply to your policy

You and we are free to choose the laws that apply to this policy. Unless you tell us otherwise in writing before the **period of insurance** starts, this policy will be governed by the laws of England and Wales and subject to the exclusive jurisdiction of the courts of England.

Unless you and we agree otherwise in writing, all communications relating to the policy will be in English.

Contacting 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 as follows:

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

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

When you make a claim, it is very important that you meet all of the requirements of the policy, particularly claim condition 1–'Reporting a claim'.

If you do not keep to the other conditions in the policy we may not pay part or all of your claim.

Making a complaint

We are committed to providing the highest standards of customer service and treating our customers fairly. If you have a complaint, contact the person who arranged this insurance for you or contact us at:

Customer Experience Manager
HSB Engineering Insurance Limited
Chancery Place
50 Brown Street
Manchester M2 2JT
Telephone: +44 (0) 330 100 3433 (Calls to this number are charged at the same standard landline rate as calls to 01 or 02 numbers.
Email: complaints@hsbeil.com

Our aim is to resolve complaints as soon as possible. If we are able to resolve the complaint within three days we will send you a summary resolution communication (SRC) to confirm the complaint has been resolved.

If the complaint takes longer than three days to resolve we will:

- confirm this within five business days;
- pass it to our complaints team to be reviewed; and
- do our best to resolve your complaint within four weeks. If we cannot, we will write to you and let you know when we will be able to give you a final response.

If we cannot resolve your complaint within eight weeks, or you are not happy with our final response, you may be able to complain to the Financial Ombudsman Service (FOS).

The FOS is an independent organisation which may be able to review your complaint for you.

You can contact the FOS at:

The Financial Ombudsman Service
Exchange Tower
London E14 9SR
Telephone: 0800 023 4567
Website: www.financial-ombudsman.org.uk

The FOS's service is available to individual policyholders as well as charities, trustees and small businesses with an income or assets within set limits. You can get more information from us or the FOS.

If you make a complaint to the FOS, this may affect your right to take legal action against us.

Making any other enquiry

If you have any questions about the policy or your cover, or you require any additional support, please contact the person who arranged the insurance or contact us.

You can find the contact details for your local HSBEIL office on the website at www.hsbeil.com.

Definitions

Where the words below are printed bold in this document or the schedule, they have the meanings shown here.

Act of terrorism
An act committed by, or threat made by, any person or group (whether acting alone or in connection with any organisation or government) for political, religious, ideological or similar purposes, including to influence any government or frighten the public.

Business
Your business activities as specified in the 'Business description' shown in the schedule.

Business income
This means:

- the amount of net income (profit or loss before taxes) which you would have earned after the **time excess** if the **cyber event** had not happened; and
- normal operating expenses that continue, including ordinary payroll.

Computer system
Any electronic device that connects to the internet or to other electronic devices and any associated **data**, software, programs, websites, intranet or extranet sites and computer networks, but not including equipment held as stock or which you have manufactured and is intended for sale or repair in the course of your **business**.

Computer virus
Any malware, program code or programming instruction designed to have a damaging effect on a **computer system**.

Contaminant
An impurity resulting from the mixture or contact of a substance with a foreign substance, including mould, mildew, fungus, spores, diseases, viruses or microorganism of any type, nature, or description.

Cyber action
The use of a **technology system** by, or on behalf of, a **state** to disrupt, deny, degrade, manipulate or destroy information in a **technology system** to hinder, defend against civil war, insurrection, rebellion, or revolution within that **state**.

Cyber event
This means:

- 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.

Cyber operation
The use of a **technology system** by, or on behalf of, a **state** to disrupt, deny, degrade, manipulate or destroy information in a **technology system** of, or in, another **state**.

Damage
Total or partial loss, damage, destruction, breakdown or corruption.

Damages
This means:

- financial compensation you have to pay, except for fines, penalties, liquidated damages (agreed damages or penalties you have to pay under a contract), punitive or exemplary damages (extra damages to punish you) or aggravated damages (more severe damages to reflect the seriousness of an offence); or
- third parties' costs and expenses you have to pay as a result of a claim being brought against you.

Data
Facts, concepts, information, ideas, text, recordings and images which are converted to a form which can be processed by **computer systems**, but not including software and programs.

Data privacy obligations
Legal obligations relating to securing, managing and preventing unauthorised access or use of **data**, and arising under:

- relevant data-protection regulations anywhere in the world associated with the confidentiality of, access to, control of and use of **personal data** which are in force at the time you discover you have failed to keep to your data privacy obligations;
- guidance from the Information Commissioner's Office or similar organisations worldwide;
- the Payment Card Industry Data Security Standard or other contractual obligations relating to handling credit-card and debit-card information;
- privacy statements and confidentiality agreements.

Defence costs
Cost and expense we agree to in writing for investigating, settling or defending a claim against you.

Denial of service attack
Malicious and unauthorised attack which overloads any **computer system**.

Directors and officers
Directors, officers, principals, partners or members while they are employed by you and under your control in connection with the **business**.

Definitions

Employee
This means any:

– person employed, borrowed or hired by you, including apprentices;

– labour master or labour-only subcontractor (or a person supplied by any of them);

– self-employed person;

– person taking part in any government or otherwise authorised work experience, training, study, exchange or similar scheme;

– person doing voluntary work for you; or

– person supplied to you under a contract or agreement which states that they are in your employment;

when they are working for you in connection with your **business**, but not including your **directors and officers**.

Excess
The 'Excess' shown in the schedule, which is the amount of your claim that we will not pay. Please note 'excess' does not apply to section 1 - Cyber incident response services under 'What we will pay for'.

Hacking
Unauthorised or malicious access to any **computer system** by electronic means.

Incident response case manager
A person assigned by us will assess the situation to determine whether a cyber event has occurred and will assist you by providing expert support in managing and mitigating the incident.

Infectious agent
Any transmissible bacterium, microorganism, virus or other pathogen that induces or is capable of inducing an infectious disease.

Indemnity period
The period during which you suffer a loss of **business income** or have to pay extra costs, starting on the date of the **cyber event** and ending no later than the last day of the **indemnity period** shown in the schedule.

Loss
Any loss, damage, liability, cost or expense of any kind.

Occurrence
One event or a series of events arising out of or in connection with the same cause, source or event.

Pandemic
A widespread outbreak of a human infectious disease, into at least three countries on two different continents.

Pandemic impact
Any of the following if they are caused by, result from, arise out of or related to a **pandemic**:

– sickness, disability or death;

– civil or military actions or orders, including confiscation; curfews; evictions; quarantines; restricted access to buildings or other property and restricted travel;

– strikes, riots or civil commotion;

– actions taken or refused to be taken by individuals or businesses:

– any other actions, advice or restrictions put in place by either the Government or competent, local, civil or military authority in order to hinder, defend against or respond to any **infectious agent** or **pandemic** or fear or threat of an **infectious agent** or **pandemic**.

Period of insurance
The period of time, as shown in the schedule, during which you are covered by the policy, unless it is cancelled or treated as though it never existed (see 'Your responsibility to provide us with a fair presentation of the risk' under 'Important information').

Personal data
Information which could identify a person or allow identity theft or other fraud to take place.

Pollutant
Any solid, liquid, gaseous, biological, radiological, or thermal irritant or **contaminant**, including smoke, vapour, soot, fumes, acid, alkalis, chemicals, vaccines and waste (including materials to be recycled, reconditioned, reclaimed, or disposed of, as well as, nuclear materials).

Service provider
A business that you hire under a written contract to perform services on your behalf in connection with your **business**.

State
Sovereign state.

Sum insured
The amount shown in the schedule.

Technology system
Any computer, hardware, software, communications system, electronic device (including but not limited to smart phone, laptop, tablet, wearable device), server, cloud infrastructure or microcontroller including any similar system or any configuration of the aforementioned and including any associated input, output, **data** storage device, networking equipment or back up facility.

Time excess
The time period, as shown in the schedule, that we will not pay any loss of **business income** for.

War
This means:

– the use of physical force by a **state** against another **state** or as part of a civil war, rebellion, revolution or insurrection; and/ or

– military or usurped power or confiscation or nationalisation or requisition or destruction of or damage to property by or under the order of any government or public or local authority;

whether war be declared or not.

What we will pay for

1. Cyber incident response service
We will pay for the cost of an **incident response case manager** to assist you in responding (as follows) to any suspected or actual cyber incident which was first discovered during the **period of insurance** (see 'What you should do if you discover a cyber incident').

a) Technical assistance
Assessment of potential **damage** to your **computer system**.

b) Incident containment
Advice on identifying and containing the **cyber event**.

c) Impact mitigation
Support to reduce **damage**, including securing **computer systems**, changing passwords and checking for backups.

d) Ongoing support
Continued guidance and coordination of further response measures where needed.

2. Computer system damage
We will pay for the following arising as a result of a **cyber event** you first discover during the **period of insurance**:

a) Computer system restoration
The cost of investigating, reconfiguring and rectifying any **damage** to your **computer system** or the **computer system** of a **service provider**, and restoring and recreating data.

This does not include the value of **data** to you, even if the **data** cannot be restored or recreated.

b) Computer virus removal
The cost of locating and removing a **computer virus** from your **computer system**.

c) Professional assistance
The cost of hiring professional consultants to make recommendations on how to prevent your **computer system** from being infected by a **computer virus** or to prevent **hacking**.

3. Loss of business income and extra costs
We will pay for the following arising as a result of a **cyber event** you discover during the **period of insurance**:

Loss of **business income** and extra costs to prevent or reduce the disruption to the functions carried out by your **computer system** during the **indemnity period**.

4. Cyber crime
We will pay for the following which you first discover during the **period of insurance**:

a) Fraud
Your financial loss

– following **hacking** that results in fraudulent input, destruction or modification of **data** in your **computer system**, or the **computer system** of your **service provider**, leading to:

· money being taken from any account;
· goods, services, property, title deeds or financial benefit being transferred; or
· any credit arrangement being made;

but excluding **hacking** by **directors and officers** or **employees**;

– resulting from you transferring funds from your account to that of a third party as a direct result of a fraudulent electronic communication;

as long as you have not received any benefit in return, and you cannot recover the loss from a financial institution or other third party.

We will also pay the cost of proving that transactions are fraudulent and that contracts or agreements were entered into fraudulently.

b) Telephone hacking
Your liability to make any payment to your telephone **service provider** as the result of **hacking** into your **computer system**.

c) Cyber ransom
The cost of responding to, and with our written agreement the payment of a ransom demand, if anyone has or threatens to:

– disrupt your **computer system** by introducing a **computer virus**, or to initiate a **hacking** attack or **denial of service attack** against you;

– release, publish, corrupt, delete or alter your **data** if this would cause you harm or **damage** your reputation;

as long as you can demonstrate that you have reasonable grounds to believe that the threat is not a hoax, and you have reported it to the police.

What we will pay for

5. Data-breach expense
If during the **period of insurance** you first discover that you have failed to keep to your **data privacy obligations** in the course of your **business**, we will pay the following:

a) Professional assistance
The cost of hiring professional legal and forensic information-technology services to investigate and tell you how you should respond.

b) Notification costs
The cost of informing affected parties, the **data** privacy regulator and other relevant third parties or organisations worldwide.

c) Customer support
The cost of providing the following support services to affected parties as the result of you failing to keep to your **data privacy obligations**:

- Credit file monitoring, identity theft assistance and helping the affected parties to correct their credit records and take back control of their personal identity;
- Providing a helpline to respond to enquiries after informing affected parties.

These services will only be provided for 12 months, and only if:

- the **data privacy obligations** you have failed to keep to relate to **personal data**; or
- you must provide the relevant service under your **data privacy obligations**.

d) Public relations
Public-relations and crisis-management expenses, if we have given our written permission, for communicating with the media, your customers and the public to minimise damage to brands and business operations, and any damage to your reputation.

6. Cyber liability
For the purposes of 6 – Cyber liability, references to 'you' also mean any of your **employees** or **directors and officers**.

We will pay **damages** and **defence costs** arising from a claim first made against you during the **period of insurance** and in the course of your **business** as a result of:

a) Data privacy
You or your **service provider** failing to secure, or prevent unauthorised access to, publication of or use of **data** (including any inadvertent interference with any right to privacy or publicity, breach of confidence or your **data privacy obligations**).

If you have failed to meet your **data privacy obligations** we will also pay fines and penalties if insurable under applicable law.

b) Computer virus transmission
You unintentionally transmitting, or failing to prevent or restrict the transmission of, a **computer virus**, **hacking** attack or **denial of service attack** from your **computer system** to a third party.

c) Defamation and disparagement
Loss of reputation (including that of a product) or intellectual property rights being infringed (broken, limited or undermined) as a result of:

- the content of any emails distributed by your **computer system**;
- the content of your website;
- online promotional marketing material; or
- other **data** processed or distributed by your **computer system**.

Extra cover

The extra cover items shown below are included within your sum insured.

1. Accountants' fees
We will pay the cost of you providing the information we need to work out the amount we should pay, as a result of:

- extra staffing costs; and
- extra fees charged by your usual auditors or accountants.

2. Avoiding corruption
If we have agreed in writing:

- we will pay the cost of locating and removing a **computer virus** from your **computer system** which has not necessarily caused any **damage** or disruption; and
- where a **computer virus** or **hacking** attack has affected your **computer system** during the **period of insurance**, we will pay the cost of hiring professional consultants to make recommendations on how to prevent your **computer system** from being infected by **computer virus** or to prevent **hacking**.

3. Fines and penalties
Following a claim against you, we will pay fines, penalties, liquidated damages (agreed damages or penalties you have to pay under a contract) and **defence costs** which you become legally obliged to pay as the result of you not keeping to your **data privacy obligations**, except for fines and penalties which you cannot insure against by law.

4. Investigation cost
If we accept a claim for **damage** or other loss, and we agree in writing, we will pay the cost of investigating possible repair, replacement or restoration.

5. Loss-prevention measures
We will pay the cost of preventing or minimising actual or expected **damage** or other loss covered by this policy, as long as:

- **damage** or other loss would be expected if the measures were not taken;
- we are satisfied that the **damage** or other loss has been prevented or minimised by these measures; and
- the cost is limited to the cost of **damage** or other loss which would have been caused.

The full terms and conditions of this policy apply as if **damage** or other loss covered by this policy had arisen.

6. Removing data
We will pay the cost of removing or withdrawing **data** from the internet or other source available to the public, as long as that would avoid or reduce a claim against you.

7. Security audit
If the failure to keep to **data privacy obligations** insured by this policy resulted from security weaknesses in your **computer system**, we will pay the cost of a professional consultant carrying out an audit of your **computer system** to assess the security weaknesses and advise you on how to make improvements.

8. Temporary and fast-tracked repair
If we accept a claim for **damage** or other loss, we will pay the cost of making temporary repairs and fast-tracking a permanent repair, replacement or restoration.

How much we will pay

The most we will pay for each **occurrence** is the **sum insured** including any 'Extra covers', regardless of the number of people or organisations insured by your policy.

1. Business income
Under 'What we will pay for 3' - 'Loss of business income and extra costs', the amount of loss of **business income** we pay will be based on your **business income** during the 12 months immediately before the **cyber event**, as recorded in your accounts. We will make adjustments to reflect trends and circumstances which may affect the **business income**, or which would have affected the **business income** whether or not the **cyber event** had happened. Any loss of **business income** we pay will be included within, not in addition to, the **sum insured**.

2. Defence costs
Under 'What we will pay for 6' - 'Cyber liability', any **defence costs** we pay will be included within, not in addition to, the **sum insured**.

3. Paying out the sum insured
For any **occurrence** arising in the **period of insurance** we may pay the full **sum insured** that applies.

When we have paid the full **sum insured**, for claims arising out of one **occurrence**, we will not pay any further amounts for any claims or for associated **defence costs** arising from the same **occurrence**.

Claim conditions

You must comply with the following conditions whenever you need to make a claim under the policy. If you do not meet these conditions, we will not be legally liable to pay a claim under the policy. However, we will not rely on a breach of a condition to decline liability for a claim if you can prove that the failure to keep to the relevant term could not have increased the risk of the loss which actually occurred in the circumstances in which it occurred.

1. Reporting a claim
Usually claims will be notified on your behalf by our Incident Response Team, otherwise as soon as you know about any incident or circumstance that may result in a claim that you tell the person who arranged the policy (or us), providing full details, as soon after the incident or circumstance as possible.

2. Claims co-operation
As soon as you know about any incident or circumstance that may result in a claim you must also:

- take all reasonable steps and precautions to prevent further **damage**, loss of **business income** or other loss;
- immediately tell the police about any loss or **damage** relating to crime and get a crime reference number;
- keep any **damaged computer system**, other property covered by this policy and other evidence and allow us to inspect it; and
- give us details of any other insurances you may have which may cover **damage**, loss of **business income**, **damages**, **defence costs** or other loss insured by this policy.

In addition, for any incident or circumstance that may result in a claim you must:

- immediately send us every letter, writ, summons or other document you receive in connection with the claim or circumstance, and record all information relating to a claim against you that is covered under 'What we will pay for 6' - 'Cyber liability';
- co-operate with us fully and provide all the information we need to investigate your claim or circumstance;
- tell us if you recover money from a third party (you may need to give the money to us); and
- not admit responsibility or liability, or agree to pay any money or provide any services on our behalf, without our written permission.

You must comply with the following conditions whenever you need to make a claim under the policy. If you do not meet these conditions, we may refuse to pay part or all of your claim.

3. Fraudulent claims
If you (or anyone acting for you) make a claim that you know is in any way false or exaggerated, or if any fraudulent means or devices are used in support of a claim or if any **damage** is caused by the wilful act or you are knowingly involved in the fraudulent act of another person then we shall be entitled to:

- not pay the claim;
- recover from you any sums previously paid by us in respect of the claim;
- treat this policy as being terminated with effect from the date of the fraudulent act; and
- cancel any other policies you have with us.

If the policy is treated as having been terminated on grounds of fraud, we shall:

- be entitled to refuse all liability under the policy in respect of any losses occurring after the time of the fraudulent act; and
- not be liable to refund any premiums paid under the policy.

4. Enforcing your rights
We may, at our expense, take all necessary steps to enforce your rights against any third party. We can do this before or after we pay a claim. You must not do anything before or after we pay your claim to affect our rights and you must give us any help and information we ask for.

You must take reasonable steps to make sure that you protect your rights to recover amounts from third parties.

5. Controlling defence
We can, but do not have to, take control of investigating, settling or defending any claim made against you. We would take this action in your name. If necessary, we will appoint an adjuster, solicitor or any other appropriate person to deal with the claim. We may appoint your solicitor, but only on a fee basis similar to that of our own solicitor, and only for work done with our permission in writing. We will only defend claims if we think that there is a reasonable chance of being successful, and after taking the costs of the defence into account.

6. Other insurances
If there is any other insurance covering your claim, we will only pay our share.

7. Salvage and recoveries
If you have made a claim and you later recover money from a third party, you must tell us immediately. If we have paid the claim, you may have to give the money to us.

If we have paid a claim and we then recover money from a third party, we will give you any proceeds above the amount we paid you in connection with the claim.

Any amount due from you or us must be paid as soon as reasonably possible.

General conditions

You must comply with the following conditions whenever you need to make a claim under the policy. If you do not meet these conditions, we may refuse to pay part or all of your claim.

1. Alteration in risk
Your cover will not be affected by any act, failure to act or change in circumstance which increases the risk of **damage**, loss of **business income** or a claim for **damages** or other loss covered by your policy and which you could not have known about or controlled.

As soon as you (or anyone acting for you) become aware of any act, failure or change in circumstance which may affect the policy, you must tell us as soon as possible and keep to any extra terms and conditions we set. This applies to any change of circumstance which arises, whether before or during the **period of insurance**, including before we renew your policy.

2. Contracts (Rights of Third Parties) Act 1999
Any person or company who is not named in the schedule has no right under the Contracts (Rights of Third-Parties) Act 1999 (or any other law) to enforce any term of the policy.

3. Data backup
You must back up original **data** at least every 7 days.

If a **service provider** processes or stores **data** for you, you must make sure that the terms of the contract between you and the **service provider** allow **data** to be backed up in line with this condition.

You must take precautions to make sure that all **data** is stored safely.

If you have failed to keep to this condition, we may still pay a claim if you can show that formal procedures are in place to keep to this condition and that the failure was an accidental oversight or as a result of circumstances beyond your control.

4. Defence software
Your **computer system** must be protected by a virus-protection software package which is:

– licensed to you; and

– updated at least every 28 days.

Your **computer system** must also be protected by a firewall on all external gateways to the internet, and that firewall must be maintained.

5. More than one insured
If more than one 'Insured' is named in the schedule, the first named insured will receive all notices and agree any changes to the policy and will be treated as acting for all the named insureds. We will not remove any named insured without their permission.

For any claim, the total amount we will pay will not be more than the **sum insured**, regardless of the number of people or organisations insured by the policy.

6. Paying the premium
You must pay the premium on or before the start of the **period of insurance** or on dates agreed by us.

If you do not pay a premium on time, we may cancel the policy (see 'Our rights to cancel your policy' under 'Important information').

7. Protecting data
You must make sure that the appropriate procedures are in place for disposing of and destroying **computer system** and hard copy files in order to protect **data**.

8. Reasonable care
You must:

– make sure that your **computer system** is maintained, inspected and tested as recommended by the manufacturer;

– keep a record of all maintenance and **data** back-up procedures and maintenance carried out, and let us check those records;

– take all reasonable steps and precautions to prevent or reduce **damage** or other loss covered by this policy; and

– not continue to use **computer system** after **damage**, unless we have given our written permission.

If you do not keep to this condition we may:

– refuse to pay part or all of your claim; and

– cancel your policy (see 'Our rights to cancel your policy' under 'Important information').

9. Tax
Any claim we pay will not include Value Added Tax (VAT), unless you cannot recover part or all of the VAT you have paid.

What we will not pay for

We will not pay for any claim, cost or loss caused by or resulting from the following:

1. Associated companies or other insured parties
Any claim brought against you by:

– another person named as 'insured' in the schedule;

– any of your parent or subsidiary companies; or

– any company which you are a director, officer, partner or employee of and have a financial interest in.

However, we will pay for any claim brought against you by your **employees** or **directors and officers** as a result of you failing to keep to your **data privacy obligations**. We will not pay any more than an unrelated third party would have received under the same circumstances.

2. Authority actions
Any action or prosecution against you by any statutory or local government agency, body or authority or professional or trade licensing organisation acting in its regulatory or official capacity.

3. Bodily injury
Any actual or alleged personal injury suffered by any person including but not limited to bodily injury, psychological harm, emotional distress, anguish, trauma, illness, an ailment or death.

This exclusion shall not apply in respect of **damages** and **defence costs** for psychological harm, mental anguish or emotional distress arising from a claim under 'What we will pay for 6' - 'Cyber liability'.

4. Circumstances before your policy started

– Circumstances which existed before any cover provided by this policy started, and which you knew about.

– Claims or circumstances which you have already reported, or which you should have reported, to a previous insurer before the **period of insurance**.

5. Confiscation
Your property being confiscated or **damaged** by, or under the order of, any government, public or police authority, other than:

– to protect life or prevent damage to property; or

– as the result of a regulatory investigation after you have failed, or allegedly failed, to keep to your **data privacy obligations**.

6. Credit-card or debit-card fraud
Under 'What we will pay for 4' - Cyber crime' - any financial loss resulting from actual or alleged fraudulent use of credit card or debit card.

7. Deficiency or improvements
The cost of correcting any failings in procedures, systems or security.

8. Deliberate act of a utility supplier
Loss of **business income** or any other cost resulting from a deliberate act or decision of a gas or electricity supplier, grid operator or telecommunications operator, except where that act or decision was necessary to protect life or prevent **damage** to property.

9. Deliberate defamation or disparagement
Defamatory or disparaging statements or publications made deliberately or recklessly if it could be anticipated by a reasonable person that the statements could result in a claim against you.

10. Employer liability
You failing to keep to any obligation you have to your **employees** or **directors and officers**, unless this is specifically insured by this policy after your **data privacy obligations** have not been met.

11. Excess
The amount specified as the 'Excess' in the schedule. This does not apply to 'What we will pay for 1' - 'Cyber incident response services'.

12. External network failure
Under 'What we pay for 2 and 3' - 'Computer system damage' and 'Loss of business income and extra costs' - We will not pay for any claim, cost or loss caused by or resulting from any cost, **damages**, liability, loss or **defence costs** arising from or in connection with failure or interruption of any gas or water supply, electrical power supply network or telecommunication network not owned and operated by you. This exclusion shall not apply to any cost or loss caused by or resulting from physical damage, if otherwise insured by your policy, to the gas or water supply, electrical power supply network, telecommunication network or other property.

Telecommunication networks include satellite networks, but are not limited to, the internet, internet service providers, Domain Name System service providers, cable and wireless providers, internet exchange providers, search engine providers, internet protocol networks (and similar networks that may have different designations) and other providers of telecommunications or internet infrastructure.

13. Extortion or ransom
Any extortion, blackmail or ransom payments or demands, other than in connection with cover provided by 'What we will pay for 4' - 'Cyber crime'.

14. Financial reporting
Any mistakes in financial statements or representations concerning your **business**.

15. Fines and penalties
Any fines, penalties, punitive or exemplary damages (extra damages to punish you) other than those specifically covered in extra cover 'Fines and penalties'

16. Fraudulent credit applications
Any financial loss resulting from a fraudulent application for credit or the provision of false details in applying for credit or opening an account with you.

17. Indirect loss
Penalties you have to pay under a contract for any delay or in connection with guarantees of performance or efficiency.

What we will not pay for

18. Infectious agents and pandemics
Any loss, **damage**, cost or expense caused by, either directly or indirectly, in connection with, or any action taken to hinder, defend against or respond to any **infectious agent**, **pandemic** or **pandemic impact** or the fear or threat (whether actual or perceived) of any **infectious agent**, **pandemic** or **pandemic impact**.

This exclusion applies regardless of any other cause or event that in anyway contributes concurrently or in any sequence to the loss, cost or expense, and regardless whether or not there is any declaration of an outbreak of a **pandemic** by the World Health Organisation or any authorised national or international body or legal jurisdiction.

19. Intentional acts
Any intentional act, or failure to act, by you or your **directors and officers**, unless the act or failure to act is a measure to prevent or minimise injury, **damage** to your **computer system**, loss of **business income** or a claim for **damages**.

20. Legislation and regulations
You actually or allegedly breaking any taxation, restraint of trade, competition or anti-trust law or regulation.

21. Normal upkeep
The cost of normal **computer system** maintenance.

22. Nuclear risks
We will not pay for any loss, **damage**, liability, cost or expense of whatsoever nature directly or indirectly caused by contributed to by or arising from:

- ionising radiation from, or contamination by, radioactivity from any nuclear fuel or nuclear waste, or from burning nuclear fuel.
- the radioactive, toxic, explosive or other dangerous properties of any nuclear installation, reactor or other nuclear equipment, or any nuclear part of them.
- any weapon or device using atomic or nuclear fission, fusion or similar reaction, or radioactive force or material.
- the radioactive, toxic, explosive or other dangerous properties of any radioactive material.

23. Patent
Infringement of any patent without the patent holders permission.

24. Pollution and contamination
Any cost, **damages**, liability, loss or **defence costs** arising from or in connection with:

- the presence of **pollutants** or a **contaminant**; or
- the actual discharge, dispersal, release or escape of **pollutants** or a **contaminant**, or
- any direction or request to test for, monitor, clean up, remove, contain, treat, detoxify, neutralize in any way respond to or assess the effects of **pollutants** or a **contaminant**.

25. Product liability or professional indemnity
Goods, products or software you have sold, supplied, manufactured, constructed, installed, maintained, repaired, altered or treated, or any inadequate or incorrect advice or services you have provided.

26. Property damage
Any cost, **damages**, liability, loss or **defence costs** arising from or in connection with any physical **damage** to any tangible property, unless otherwise covered under 'What we will pay for 2' - 'Computer system damage'.

27. Sanction limitation
We will not make any payment under the policy if doing so would expose us to any sanction, prohibition or restriction under any United Nations resolutions, or the trade or economic sanctions, laws or regulations of the European Union, United Kingdom or United States of America.

28. Telecommunications systems
Atmospheric or environmental conditions causing temporary interference with any satellite signal.

29. Terrorism
- Any **act of terrorism**, regardless of any other cause or event contributing to the **damage**, loss of **business income** or other loss.
- Civil commotion in Northern Ireland.
- Any action taken to control, prevent, suppress or in any way deal with any **act of terrorism**.
- **Computer virus**, **hacking** or **denial of service attack** will not be regarded as an **act of terrorism**.

30. Time excess
Loss of **business income** arising during the **time excess**.

31. Trading risk
Your commercial decision to stop trading, or the decision of a **service provider**, customer or supplier of yours to stop or reduce trade with you or restrict services.

What we will not pay for

32. War
Any **loss** directly or indirectly occasioned by, happening through or in consequence of **war**, a **cyber operation** or a **cyber action**.

We shall have the burden of proving that this exclusion applies.

*Attribution of a **cyber operation** to a **state**:*

- The primary but not exclusive factor in determining attribution of a **cyber operation** shall be whether the government of the **state** (including its intelligence and security services) in which the **technology system** affected by the **cyber operation** is physically located attributes the **cyber operation** to another **state** or those acting on its behalf.
- Pending attribution by the government of the **state** (including its intelligence and security services) in which the **technology system** affected by the **cyber operation** is physically located, we may rely upon an inference which is objectively reasonable as to attribution of the **cyber operation** to another **state** or those acting on its behalf. It is agreed that during this period no **loss** shall be paid.
- In the event that the government of the **state** (including its intelligence and security services) in which the **technology system** affected by the **cyber operation** is physically located either:
  · takes an unreasonable length of time to, or
  · does not, or
  · declares it is unable to

Attribute the **cyber operation** to another **state** or those acting on its behalf, it shall be for us to prove attribution by reference to such other evidence as is available.

*Attribution of a **cyber action**:*

- The primary but not exclusive factor in determining attribution of a **cyber action** shall be statements by widely recognised international bodies (such as the United Nations) or alliances (such as the North Atlantic Treaty Organisation).
- Pending attribution by a widely recognised international body or alliance, we may rely upon an inference which is objectively reasonable as to attribution of the **cyber action** to a **state** or those acting on its behalf. It is agreed that during this period no **loss** shall be paid.
- In the event that the widely recognised international body or alliances:
  · takes an unreasonable length of time to, or
  · does not, or
  · declares it is unable to

Attribute the **cyber action** to a **state** or those acting on its behalf, it shall be for us to prove attribution by reference to such other evidence as is available, such as consensus opinion within relevant expert communities, such as the cyber security industry.

33. Your insolvency or bankruptcy
Any loss, **damage**, liability, cost or expense of whatsoever nature directly or indirectly arising out of or in connection with your insolvency or bankruptcy.

© 2026 HSB Engineering Insurance Limited. All rights reserved.

HSBEI 2054-0526-4

Picture credits: Getty Images

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.

Policy wording reference: POL-UKG-CYB-003-ETR-2.00

www.hsbeil.com

HSB

A Munich Re company