CyberSafe Insurance

Insurance Product Information Document

This insurance is provided by NMU (Specialty) Ltd, which is registered in England. NMU is authorised and regulated by the Financial Conduct Authority, reference number 310539.
The following summary does not contain the full terms and conditions of the contract, which can be found in your policy documentation. The sums insured and limits of liability are shown in your policy schedule.

What is this type of insurance?

NMU CyberSafe Insurance is designed to offer protection from cyber risks which could be damaging to your business and reputation.

What is insured?

Some elements of the cover are optional, these are noted below. Please refer to your policy documentation for confirmation of the cover you have selected.

First Party Cover

Cyber Response

✓ The costs of identifying the cause of a cyber event, cyber extorsion or data breach and making recommendations as to how this might be terminated or mitigated.

Cyber Restoration

✓ Following a cyber event or data breach, the costs to:

- replace, restore or repair data and software that has been lost or damaged;
- replace or repair hardware that has been damaged.

Cyber Expense

✓ Following a data breach, the costs of:

- collation of information and notification of the breach to affected parties and/or the Supervisory Authority;
- the purchase of identity and credit theft insurance for affected parties;
- an expert to provide advice to minimise adverse publicity and reputational harm.

Court Attendance Costs

✓ Compensation for attending court as a witness in connection with a claim against you.

Cyber Extortion

✓ Following a credible threat or ransom demand:

- the costs of an expert to provide advice to minimise adverse publicity and reputational harm;
- the value of any ransom paid under duress.

Business Interruption

✓ Following a cyber event or data breach loss of income and increased cost of working during the interruption period, but not exceeding a maximum period of six months, resulting from:

- interruption or interference to your business;
- cancellation of contracts by customers due to reputational harm.

Cyber Crime (optional)

✓ Financial loss arising from:

- the transfer of funds to a third party as a direct result of a fraudulent misleading instruction;
- a fraudulent input, destruction or modification of data in your computer system resulting in;
  - money being taken from any account;
  - goods, services, property or financial benefit being transferred;
  - any credit arrangement being made; or
  - your customer transferring to an unauthorised third party money, goods, services or property which you were entitled to receive.
- your liability to make any payment to your telephone service provider as the result of a cyber attack on your computer system.

What is insured? (continued)

Third Party Claims

Cyber Liability

✓ Any award of damages and defence costs following an actual or alleged data breach.

Network Security Liability

✓ Any award of damages and defence costs following a cyber event which results in:

- damage to, destruction of, alteration of, unauthorised access to or disclosure of data stored on a third party computer system;
- interruption or degradation of services of a third party computer system.

Media Liability

✓ Any award of damages and defence costs following:

- defamation including libel, slander, trade or character disparagement;
- invasion or interference with the right to publicity or the right to privacy;
- misappropriation of any name or likeness for commercial advantage;
- infringement of intellectual property rights, but not patent;

which directly arises from the content of your website, emails or social media.

Payment Card Industry Liability (optional)

✓ If a payment service provider brings a claim against you for an actual or alleged breach of any contractual duty under a payment card processing agreement:

- contractual fines or penalties arising out of your failure to comply with PCI Data Security Standards, including card reissuance costs and card fraud recoveries;
- costs of a mandatory audit in order to demonstrate compliance with PCI Data Security Standards;
- defence costs.

What is not insured?

✗ Bodily injury, mental injury or death. This does not apply to any third party claim seeking compensatory damages for mental anguish or distress.

✗ Damage or loss of use of tangible property.

✗ Loss of value of data.

✗ Guarantee, warranty, contractual term or liability assumed or accepted by you under any contract or agreement.This does not apply to any Payment Card Industry Liability, if covered by your policy.

✗ Money or securities, or the decrease in financial value of an asset. This does not apply to any financial loss arising out of Cyber Crime, if covered by your policy.

✗ Fraudulent or reckless collection and/or processing of personal data by you without the permission of the owner of the data.

✗ Your use of illegal or unlicensed software.

✗ Failure of infrastructure other than your computer system.

✗ Overloading of bandwidth connections or webservers unless as a direct result of a cyber attack.

✗ Spam and/or unsolicited marketing communications knowingly sent by you.

Are there any restrictions on cover?

- ! An excess, being the part of a claim you are responsible for, may apply to your policy.
- ! A waiting period, being the period for which there is no cover, may apply in respect of business interruption losses.
- ! The policy will contain financial limits on the maximum values we insure.
- ! Your policy may contain other restrictions, please refer to your policy documentation.

Where am I covered?

- ✓ The policy is available for businesses operating within the United Kingdom.

What are my obligations?

- You must keep confidential the cover for cyber extortion unless disclosure to law enforcement authorities is required.
- You must provide us with honest, accurate and complete information – whether you are taking out, renewing or making changes to your policy.
- You must observe and fulfil the terms and conditions of your policy as failure to do so could affect your cover.
- You must pay the premium.
- You should inform us without delay of any material changes to your risk. If you do not inform us about a change it may affect any claim you make or could result in your insurance being invalid. Following a change we may need to apply additional terms and conditions, which you must observe, or require you to pay an additional premium. You may also need to take action, if so we will advise you.
- In the event of a cyber event or data breach you must notify the Breach Response Provider named in your policy as soon as practicable.
- For all other claims you must notify us as soon as practicable.
- You should take all reasonable steps to prevent further loss or damage.

When and how do I pay?

- Typically, annually at inception. Your premium may be subject to adjustment on expiry, based on a declaration of actual values.

When does the cover start and end?

- Typically, the policy is for a period of 12 months commencing on the date stated in the policy schedule.

How do I cancel the contract?

- ✓ You may cancel this policy at any time during the period of insurance by advising us.