INSURANCE COMPANY
LEV INS
ACTIVE SECURITY

cyberlev ins

INSURANCE POLICY
CYBER LEV

00 800 10 200 000
office@cyberlevins.com
www.cyberlevins.com

1. Introduction

Cyber Lev Insurance provides and pays for the services of a cyber expert, together with certain other payments, to help you recover from a cyber threat, cyber-attack, cyber theft which has been discovered during the period of insurance, or a third party liability claim in relation to your compromised office computer systems which has been made against you during the period of insurance, subject to the conditions and exclusions of this insurance and the payment of the premium. The services provided and how much we will pay are set out in Section 4. “What you are covered for”.

2. How to make a claim

In the event of a claim, please call the claims handler on the telephone number specified in the schedule.

3. Definitions

The following words shall have the same meaning wherever they appear in this policy.

Cyberattack means a deliberate digital attack designed to damage, delete, corrupt, destroy or disrupt your office computer system or your digital assets including computer virus and hacker attack.

Digital Assets means software and any electronic data that is stored on/or within your office computer system.

Third Party Liability means a written demand for compensation, injunctive or other relief made against you by a third party for damages sustained and arising directly from a hacker gaining unauthorised access to the content of your office computer system.

Cyber expert means any cyber security specialist appointed by the claims handler to provide you with cyber security expert help.

Cyber theft means any theft of your digital assets by a hacker.

Cyber threat means any threat from a third party to damage, delete, corrupt, destroy or disrupt by any means your office computer system or your digital assets.
Hacker means a third party who maliciously targets you and gains unauthorised access to your office computer system solely by circumnavigating the security systems in place to protect against such unauthorised access.
Office means your office premises, used by you for commercial/professional activities at the address stated in the schedule.
Office computer system means any computer, hardware, software that connects to your office internet, owned by you and used for commercial/professional purposes and is located at your office.
Incident means a cyber threat, cyber attack, cyber theft or third party liability claim.
Period of insurance means the period set out in the schedule.
Claims handler means the appointed claims representative of the Insurer responsible for settling claims according to this Insurance Policy. Details of the claims handler can be found in the schedule.
We, our, us, insurer means Insurance Company Lev Ins AD authorized and regulated by the Financial Supervision Commission of Bulgaria.
You, your means the entity named as the Insured in the schedule.

4. What you are covered for:
4.1. Cyber threat or Cyber attack
If you are the victim of a cyber threat or cyber attack during the period of insurance we will:
4.1.1 Provide expert help as follows: Initial expert advice and assistance through our telephone based, 24/7

4.1.1 Provide expert help as follows:
Initial expert advice and assistance through our telephone based, 24/7 helpline.

Thereafter, we will provide further advice and expert help either by telephone or remote access software, to where possible:

- investigate the cyber threat or cyber attack and identify its nature;
- restore your office computer system and your digital assets utilising your own back ups.

We will provide up to 25 hours of expert help.

4.1.2 Pay you the reasonable and necessary:

- cost of repairing or replacing your office computer system, where our expert help provided at 4.1.1 has been unable to resolve the cyber attack, up to the maximum limit stated in the schedule;

In order for the insurer to pay you the afore referenced reasonable and necessary costs, under this present section, without excluding any of the conditions as stated here below in Section 6. "Conditions", you shall have to have installed or have provided a remote access in order for it to be installed a recommended by the insurer EDR (Endpoint detection and response) Protection Security Solution. (installation can be performed by you or a cyber expert of ours).

We will reimburse you up to the maximum limit as stated in your schedule in total for the period of insurance.

It is imperative that should you become a victim of a hacker attack, you notify the Police and the Claims handler immediately.

4.2. Cyber theft
If you are the victim of cyber theft during the period of insurance we will:

4.2.1 Provide expert help as follows:
Initial expert advice and assistance through our telephone based, 24/7 helpline. Thereafter, we will provide further advice and expert help by telephone, to where possible;
We will provide up to 25 hours of expert help.

4.2.2 Expert advice to prevent or minimize potentially adverse effects of a newsworthy cyber event.

4.2.3 Advise on notifying data subjects who may be affected by the breach.

4.3. Restriction of Access
Advise on circumventing the potential restriction or impediment of access to your office computer systems.

In order for the insurer to provide you with the afore referenced expert support, under this present section, without excluding any of the conditions as stated here below in Section 6. "Conditions", you shall have to have installed, or have provided a remote access in order for it to be installed, a recommended by the insurer EDR (Endpoint detection and response) Protection Security Solution (installation can be performed by you or a cyber expert of ours).

4**.4.** Third party liability
If you are required to settle a claim or a judgement award arising from a third-party liability claim first made against you during the period of insurance we will:
We will provide up to 25 hours of expert help.

4.4.1 Assist you in defending a claim or judgement up to a sublimit of 20% of the maximum limit stated in the schedule. It is obligatory for you to adhere to the claim handler's suggestions and solutions.

5. What you are not covered for:
We do not cover:

5.1. physical loss or damage to tangible property, other than damage to your office computer system from a cyber attack or by a hacker;

5.2. loss arising from the failure of services from any third party service provider;

5.3. any loss or damage or liability whatsoever that is coincidental to the purposes of your trade, business or profession;

5.4. the costs or retrieving, repairing or replacing any of your personal digital data including but not limited to photographs, videos or music;

5.5. any cause that precedes the start of this policy and you know of or reasonably should have known would be likely to lead to a covered claim or loss;

5**.6.** any costs arising from any kind of business interruption;

5.7. any costs arising from regulatory fines and penalties including but not limited to GDPR violations, data protection regulations, etc.

5.8. in no event shall the Insurer be responsible or liable for any failure or delay in the performance of its obligations arising out of or caused by, directly or indirectly, forces beyond its control, including, without limitation, strikes, work stoppages, accidents, acts of war or terrorism, civil or military disturbances, nuclear or natural catastrophes or acts of God, and interruptions, loss or malfunctions of utilities, communications or computer (software and hardware) services; it being understood that the Insurer shall use reasonable efforts which are consistent with accepted practices in the insurance industry to resume performance as soon as practicable under the circumstances.

5.9. any Confiscation, expropriation, forced nationalization, damage / removal of property under order of a current government or authority; confiscation, imposed as a punishment or sentence for a crime committed under any Penal Code and deactivation or blocking of access to your digital assets or office computer systems, or attributable to any errors or omissions pertaining to your professional conduct;

5.10. any kind of cyber risk which is not specifically mentioned in this current Insurance Policy, or endorsements thereof, under the present conditions;

5.11. any incident occurring outside of the country of where your business is located. Cover extension for European Union is available upon request;

5.12. infringement of any intellectual property rights.

6. Conditions

Pre-Conditions of liability to provide service and payment:
It is a pre-condition of the Cyber Lev Insurance Policy to provide the services and payments stated hereunder that:

a. You shall have paid the premium stated in the schedule as at the date of any incident;

b. You must ensure that password protection is enabled, all software updates are applied within 90 days of their availability, that all firewalls are active and anti-virus software is current and active on all computers, portable devices used, owned or controlled by you.

c. In order for the insurer to provide the payment under sections 4.1.2 and 4.3., without excluding any of the conditions as stated here in the present Section 6. "Conditions", you shall have to have installed, or have provided a remote access in order for it to be installed, a recommended by the insurer EDR (Endpoint detection and response) Protection Security Solution (installation can be performed by you or a cyber expert of ours).

d. You must provide notice to the Police and to the Claims Handler of any incident discovered during the period of insurance as soon as you can. For the purposes of this condition:

i. 'discovered' shall mean the knowledge of you or anybody employed by you;

ii., notice must be provided to the Claims Handler via the emergency telephone line specified in the schedule.

e. You shall not admit to any liability for or settle any claim without our prior written consent. If you do, we may deny or reduce any payment we make under the Policy.

7. Subrogation

It is hereby understood that the Insurer subrogates to the rights of the Insured in any event that payment of costs or reimbursement is provided.

8. Fraud

If you, or anyone on your behalf, tries to deceive us by deliberately giving us false information or making a fraudulent claim under this Cyber Lev Insurance Policy, then we shall be entitled to serve notice to terminate this Insurance Policy with effect from the date of the giving of false information or making of the fraudulent claim.

We shall be entitled to retain all premium payments and shall make no payment in respect of any claim made after the date of termination. You must reimburse any payments already made under this Cyber Lev Insurance Policy in relation to any claim made after the date of termination.

9. How to make a complaint

Should you have a complaint regarding this Cyber Lev Insurance Policy, please contact the Insurer.

Complaints which cannot be resolved may be referred to the Financial Services Regulator of the country where the risk is located.
Your legal rights are not affected by this complaint's procedure.
10. Data Protection Notice.

We and the Claim Handler collect and process information about you in order to provide and administer insurance policies and to process claims.
We and the Claims Handler may record telephone calls to help monitor and improve the service provided.

11. Governing Law
Unless some other law is agreed in writing, this Cyber Lev Insurance Policy will be governed by the laws of the country where the risk is located.

12. Our promise
In return for the premium you have paid, we agree to insure you in accordance with the terms and conditions of this Cyber Lev Insurance Policy.

These General Terms and Conditions have been accepted by the Management Board of Insurance Company LEV INS AD, with company number in the Bulgarian Commercial Register 121130788, License № 98/06.01.2000, with a Protocol dated 19.03.2021.