Cyber+ Insurance Policy (Commercial)

PROSPECTUS

Magma General Insurance Limited (erstwhile Magma HDI General Insurance Company Limited) | www.magmainsurance.com | E-mail: customercare@magmainsurance.com | Toll Free: 1800 266 3202 | Registered Office: Equinox Business Park, Tower 3, Ambedkar Nagar, 2nd Floor, Unit Number 1B & 2B, LBS Marg, Kurla (West), Mumbai - 400070, Maharashtra, India. | CIN: U66000MH2009PLC460693| IRDAI Reg. No. 149 | Cyber+ Insurance Policy (Commercial) | Product UIN: IRDAN149CP0017V01201819| For complete list of details on exclusions, risk factors, terms & conditions, please read the policy documents carefully before concluding a sale. | Trade Logo displayed above belongs to Magma Ventures Private Limited and is used by Magma General Insurance Limited under license. | Chat with MIRA on our website or say “Hi” on WhatsApp No. 7208976789 (Pros.C+.ver27.11.25)

TABLE OF CONTENTS

Cyber+ Insurance Policy (Commercial)

Prospectus

1. Introduction

Cybercrime incidents have been growing steadily in India. Cybercrime cases, registered under the Indian IT Act, increased at a rate of 300 per cent between 2011 and 2014. Data shows that in January and February 2017 alone, more than 27,000 cyber security threat incidents occurred and 39 government websites were hacked. India has been ranked fourth most vulnerable country in terms of

cyber security breaches in the world in 2016. Most commonly targeted business sectors for attacks in Asia were finance (46%), manufacturing (32%), and education (9%).

Here are a few incidents of Cybercrime that affected India

- 2016 Indian Banks data breach - It was estimated 3.2 million debit cards were compromised. Major Indian banks- SBI, HDFC Bank, ICICI, YES Bank and Axis Bank were among the worst hit.
- Petya ransomware cyberattack in June had brought cyber onslaught home. The breach had forced country's largest port Jawaharlal Nehru Port Trust in Mumbai to shut operations in one of its three terminals.
- Zomato said in May that it was affected by a data breach which led to details of 7.7 million users being stolen. The leaked information, listed for sale on a Darknet market.
- Reliance Jio was also affected by a data breach; a website called magicapk.com went up last month, allowing anyone to search for personal details of Jio customers.

Cyber liability insurance coverage is designed to protect businesses from Internet-based risks. Basically the policy covers liability and expenses arising from the theft or loss of data, as well as liability and expenses arising from a breach of data security or privacy.

2. SCOPE OF COVER

The insurance cover is provided by the Insurer to the Insured in accordance with this General Section and other applicable Sections and Endorsement(s) of the Policy.

2.1. Claims against Insured

2.1.1. Claims and Circumstances

The Insurer agrees subject to the terms, limitations, exclusions and conditions of this Policy to pay any damages and costs which the Insured shall become liable to pay arising from an Information Security Breach:

a) of which the Insured first became aware during the Period of Insurance and

b) occurring during the Period of Insurance or where specifically agreed on a date on or after the Retroactive Date up until expiry of the Period of Insurance and

c) in respect of which there has been a Claim or Circumstance notified to the Insurer during the Period of Insurance.

2.1.2. Legal expenses and civil liability to fines and penalties

The Insurer shall subject to the terms, limitations, exclusions and conditions of this Policy to provide cover to the Insured for a Data Protection Breach

a) of which the Insured first became aware during the Period of Insurance and

b) occurring during the Period of Insurance or where specifically agreed on a date on or after the Retroactive Date up until the expiry of the Period of Insurance and

c) in respect of which an allegation is made against the Insured directly leading to proceedings

i. by a Regulator or other prosecuting, administrative or regulatory body of a government, state or local authority, or

ii. of a professional or disciplinary nature brought by a trade or professional body of which the Insured is a member or by which the Insured is regulated (not including the PCI Security Standards Council)

d) and the Insured is at risk of a civil liability to pay a penalty, fine, compensation or costs.

2.2. Insured's Own Losses

2.2.1. Forensic Examinations

In the event of an Information Security Breach during the Period of Insurance, the Insurer shall pay reasonable fees and expenses for a Forensic Examination conducted by the Service Provider identified in the Schedule or as agreed by the Insurer. The Forensic Examination shall mean, so far as appropriate:

a) Identification of the cause of the Information Security Breach

b) Identification of the nature and extent of the Information Security Breach

c) Making recommendations for the prevention of a future comparable Information Security Breach.

2.2.2. Notification

In the event of an Information Security Breach during the Period of Insurance, the Insurer shall pay reasonable fees and expenses for Notification by the Service Provider identified in the Schedule or as agreed by the Insurer. Notification means, so far as appropriate:

a) notification of the Information Security Breach to parties reasonably suspected by the Insured to be affected by the Information Security Breach (including identification of such parties, collation of those parties' contact information, despatch of notices, advertising)

b) notification of the Information Security Breach to the relevant Regulator where duty of notification exists

c) establishing means by which to respond to enquiries from such parties following notification (including telephone call centre costs)

2.2.3. Public Relations Advice

In the event of an Information Security Breach during the Period of Insurance that the Insured reasonably believes will cause significant harm to its reputation, the Insurer shall pay reasonable fees and expenses for the Public Relations Advice from the Service Provider identified in the Schedule or as agreed by the Insurer. Public Relations Advice shall mean, so far as appropriate:

a) monitoring public sentiment; and

b) devising and executing a public relations strategy to protect or re-establish the reputation of the Insured.

2.2.4. Identity Monitoring

In the event of an Information Security Breach during the Period of Insurance, the Insurer shall pay so far as appropriate for Identity Monitoring by the Service Provider identified in the Schedule or as agreed by the Insurer. Such cover arises where the misuse of the personal data, identity, or financial information of natural persons affected by the Information

Security Breach is reasonably suspected by the Insured, and cover continues for a period up to 12 months after the Information Security Breach. The costs of Identity Monitoring shall be agreed in advance with the Insurer. Subject to the provisions of this term, the Insurer shall not unreasonably withhold its consent to the incurring of such costs.

2.2.5. Recovery of Insured's Data and Software

In the event of a Cyber Incident during the Period of Insurance, the Insurer shall pay reasonable fees and expenses for the Recovery of the Insured's Data and Software by the Service Provider identified in the Schedule or as agreed by the Insurer. Recovery of Insured's Data and Software shall mean:

a) investigation as to whether data and software on the Insured's Network and Computer Systems can be repaired, restored or replaced.

b) the repair, restoration or replacement of data and software on the Insured's Network or Computer Systems to regain its operational state prior to the Insured Event.

2.2.6. Business Interruption

In the event that the Insured's Computer System or Network is interrupted or interfered with during the Period of Insurance as a direct result of a Cyber Incident, the Insurer shall pay to the Insured the amount of Business Interruption Loss directly resulting from such interruption or interference during the Indemnity Period subject to expiration of the Waiting Period and provided that:

a) the Cyber Incident that directly results in the interruption or interference with the Insured's Computer System or Network occurs during the Period of Insurance or where specifically agreed on or after the Retroactive Date up until the expiry of the Period of Insurance;

b) the liability of the Insurer under this Section shall be subject to the payment by the Insured of the Deductible specified in the Schedule and shall be applied against the Sum Insured including the Maximum Sum Insured;

c) all Business Interruption Loss during the Period of Insurance which is caused by the same originating cause shall be deemed a single Business Interruption Loss;

d) cover is provided only for the Insured's Network and Computer Systems located at the Insured Location(s) specified in the Schedule.

2.2.7. Theft of Electronic Money

In the event of a Cyber Incident during the Period of Insurance, the Insurer shall indemnify the insured for Electronic Money legally and beneficially owned by the Insured that is stolen which:

a) directly results from a Cyber Incident; and

b) is committed by a person acting in collusion with those responsible for the Cyber Incident;

c) is not committed by the Insured or an Employee; and is discovered by the Insured during the Period of Insurance.

2.3. Optional Sections

2.3.1. Media Liability

The Insurer agrees subject to the terms, limitations, exclusions and conditions of this Policy to pay any Loss as specifically covered by this Section arising from an Insured Event occurring during the Period of Insurance.

For the purposes of this Section, an Insured Event means:

a) libel, slander, trade libel or disparagement of a person or company, or a person or company's goods or services; or

b) infringement of copyright, title, slogan, trade name, trademark, registered name or other intellectual property rights of a person or company; or

c) plagiarism, piracy or misappropriation of ideas;

d) invasion or interference with rights of privacy or public disclosure of private matters;

e) unauthorised deep-linking, framing, data extraction or web-harvesting.

arising from the website, social media or other online presence of the Insured or a Third party supplier where such Insured Event:

i. is first known to the Insured during the Period of Insurance and

ii. occurs during the Period of Insurance or where specifically agreed on a date on or after the Retroactive Date up until expiry of the Period of Insurance and

iii. in respect of which there has been a Claim or Circumstance notified to the Insurer during the Period of Insurance.

2.3.2. PCI DSS Costs and Penalties

The Insurer agrees subject to the terms, limitations, exclusions and conditions of this Policy to pay any Loss as specifically covered by this Section arising from an Insured Event during the Period of Insurance.

For the purposes of this Section, an Insured Event means an Information Security Breach:

a) of which the Insured first became aware during the Period of Insurance and

b) occurring during the Period of Insurance or where specifically agreed on or after the Retroactive Date up until the expiry of the Period of Insurance and

c) in respect of which the Insured is subject to a PCI DSS Penalty or PCI DSS Costs by reason of non-compliance with applicable PCI DSS;

2.3.3. **Cyber Threat and Extortion**

I. In the event of a Cyber Threat and Extortion to cause an **Information Security Breach**, the **Insurer** shall pay reasonable fees and expenses of the Crisis Adviser identified in the Schedule or as agreed by the **Insurer**.

II. If so advised by the Crisis Adviser and with the prior written consent of the **Insurer,** any payment made by the **Insured** to a third party, reasonably believed by the **Insurer** to resolve or terminate the Cyber threat shall be covered.

III. The cover is provided subject to the following conditions:

a) The coverage has been kept confidential by the Insured.

b) The **Insured** has taken reasonable steps to verify its belief and reasonably believes, the threat is genuine, credible and probable.

c) The **Insured** has appointed the Crisis Adviser and provided all necessary information without delay.

d) The **Insured** or the Crisis Adviser has notified the police or, the relevant Regulator or other public investigating authorities without delay.

e) The threat has not been made by or on behalf of a government, state or public authority.

IV. The cover is subject to a Sub-Limit specified in the Schedule.

V. The fees and expenses of the Crisis Adviser shall be agreed in advance with the **Insurer**.

3. Exclusions

Save as expressly covered any Claim, Circumstance, Costs or Loss arising directly or indirectly from the following are excluded from cover:

i. Bodily Injury to any person or Property Damage.

ii. A deliberate or reckless breach of duty, contract, statute or regulation.

iii. Breach of anti-trust or competition law.

iv. Any claim by an Insured person or company against another Insured person or company.

v. Any claim against a director, officer or partner of the Insured:

   a. covered in whole or in part by a policy of insurance providing cover for the liability of directors and officers

   b. asserting breach of duty by the director, officer or partner to the Insured and/or its shareholders or members

   c. where the director, officer or partner is at risk of a civil or criminal liability to pay a penalty, fine, compensation or costs in a personal capacity.

vi. Any Computer System or Network that is not owned or operated by the Insured or operated by a Third Party Supplier.

vii. Shutdown of Computer System or Network planned by the Insured or a Third Party Supplier.

viii. Any claim arising from a Product.

ix. Any claim caused by or attributable to an act or omission of a third party to the extent that a subrogation claim against such third party is prevented by reason of an agreement with the Insured.

x. War, hostilities or warlike operations (whether war is declared or not), invasion, civil uprisings, riot, rebellion, insurrection, illegal strikes, decrees of government or state or public authorities.

xi. Terrorist activity. For the purposes of this term, terrorist activity includes actions by a person or persons whether singly or in groups for the achievement of political, religious, ethnic or ideological aims that are apt to spread fear or terror amongst the population or parts of the population in order to exert influence on a government, state, public authority or company or institution. Terrorist activity can include, but is not limited to, the use of force or violence or the threat thereof. Also excluded is any loss or expense of whatever nature directly or indirectly caused by resulting from or in connection with any action taken in controlling, preventing or suppressing terrorist activity.

xii. Any intervention, order, decree or other action of a government, state or public authority.

xiii. Unsolicited communications or sending or distribution of messages using the telephone or other media.

xiv. Unauthorised video or audio recordings.

xv. Pornographic content, advertising, prize competitions or games of chance.

xvi. The Insured's use of data or software that it is not authorised to use.

xvii. All or part of a claim to the extent that it results in an improvement to a Computer System or Network or places the Insured in a better position than prior to the event giving rise to such claim.

xviii. Any claim arising from dishonesty of the Insured.

xix. Any claim made against the Insured prior to inception of the Policy.

xx. Any claim involving a circumstance notified to an insurer prior to the inception of the Policy.

xxi. Any claim involving a circumstance of which the Insured became aware prior to inception of the Policy which the Insured knew or ought reasonably to have known had the potential to give rise to a claim.

xxii. Any claim arising directly or indirectly from the failure or interruption or outage however caused including any electrical power interruption or surge, brownout, blackout, short circuit, over voltage, or power fluctuation or outage to gas, water, telephone, wireless communications, data transmission lines, cable, satellite, telecommunications, or internet or any component thereof including hardware, software, or any other infrastructure, services, equipment or facilities whether provided to the Insured or a Third Party Supplier save where expressly covered by this Policy.

xxiii. The wear and tear, progressive or gradual reduction in performance of information technology software or systems of the Insured arising from its ageing or from the failure by the Insured or those acting on behalf of the Insured reasonably to maintain, service, update or replace the same.

xxiv. Any claim arising directly or indirectly from any current or former or prospective Employee in respect of any obligation owed by the Insured as employer including without limitation any unfair or wrongful dismissal, breach of employment contract, humiliation, harassment, discrimination or like conduct.

xxv. Any failure of the Insured to make payments under a licence agreement, royalties, payments for infringement of copyright or patent.

xxvi. Ionising radiation or contamination by radioactivity from any nuclear waste from the combustion of nuclear fuel, or the radioactive, toxic, explosive or other hazardous properties of any explosive nuclear assembly or nuclear component thereof.

4. Policyholders' obligations

The Insured shall take reasonable steps to prevent or minimise any Claim, Circumstance, Costs or Loss under this Policy.

Without limitation to this condition, the Insured shall maintain up-to-date security measures in relation to its information technology including virus scanners, firewalls, encryption systems, back-up, server protection and any other systems as may be reasonable for its Business. Where the information technology of the Insured is outsourced the Insured shall ensure that the terms of contractual arrangements that apply are adhered to and that such contracts are maintained or renewed with appropriate suppliers reflecting the needs of its Business.

5. Notification

Any notice to be given in relation to this Policy must be given in writing. This includes instantaneous means of communication provided they are permanent or retrievable.

Address for Notification:

Magma General Insurance Company Limited,
Equinox Business Park, Tower 3,
Ambedkar Nagar, 2nd Floor,
Unit Number 1B & 2B, LBS Marg,
Kurla (West), Mumbai - 400070,
Maharashtra, India.
Phone +91 22 67284800

Important Note:

The details furnished above are only a summary of product features and do not describe the entire terms, conditions and exclusions on the Policy. For further details or clarifications on the Policy contact Magma officials or your insurance advisor. We shall be pleased to furnish further details.