



Policy Summary

Angel Cyber Insurance Solution

September 2023
CYB 07/23 ANG.4



Cyber Risk Management Insurance Solution Policy Summary

The following summary does not contain the full terms and conditions of the insurance which can be found in your Policy documentation. This summary does not form part of your contract of insurance. You need to keep us informed about any changes in your circumstances, so that, in the event of a claim, you still have adequate and valid insurance cover.

Who is the Insurer?

This insurance is underwritten by AXA XL Insurance Company UK Limited, under a facility administered by Angel Risk Management Limited. AXA XL Insurance Company UK Limited is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority (Firm Reference No. 423308).

About this Insurance

In today's world, an organisation's reliance on technology and the storage and processing of data is critical. The more dependent a business is on technology, the greater the risk of a cyber event. Managing security in this rapidly changing environment is one of the main challenges facing organisations of all sizes.

A business is responsible for its own cyber security, but in the event of a cyber incident, cyber insurance can help to protect your business by providing 24 hours access to a First Response Service Provider and covering first party losses (e.g. privacy notification and crisis management costs, business interruption and increased cost of working) and third-party losses (e.g. multimedia internet liability, security and privacy liability).

When and How Do You Pay for Your Insurance?

For full details of when and how to pay, you should contact your broker.

Law and Jurisdiction

Unless specifically agreed to the contrary the policy shall be governed by English law and subject to the exclusive jurisdiction of the courts of England and Wales.

The language of the policy and all communications relating to it will be in English.

Where Are You Covered?

This insurance offers Worldwide cover excluding the USA and Canada.

Policy Duration – When Does Your Cover Start and End?

This insurance cover is valid from the start date and end date of the cover are specified in your policy schedule.

What Are Your Obligations?

- You must tell us as soon as practicably possible if you become aware about any changes in the information you have provided to us which happens before or during any period of insurance.
- When we are notified of a change we will tell you if this affects your policy. For example we may amend the terms of your policy or require you to pay an additional premium. In certain circumstances we may cancel your policy in accordance with the "Cancellation and Cooling-Off Period" section of the policy document. If you do not inform us about a change it may affect any claim you make or could result in your insurance being invalid.



Significant Features and Benefits

Provides cover for First Party Losses following a Network Compromise, Data Breach or Extortion Demand (First Party Event):

- **24 hours access to a First Response Service Provider**

In the event of a cyber incident, call the Cyber Response Hotline number stated in the policy schedule. Your call will be answered by a Crawford call centre for emergency assistance with 24/7/365 access.

- (a) Crawford will assist you in coordinating your response to a first party event and in containing a first party event and mitigate any further loss.
- (b) If required, Crawford will coordinate with pre-approved vendors including legal advice and/or with IT Specialist S-RM for assistance in determining what has been affected and how it can be contained, repaired or restored.

- **Privacy Notification and Crisis Management Costs**

Costs that you incur with the First Response Service Provider, with prior written consent from us, following a First Party Event which is first discovered during t:

- (a) legal fees in order to determine the actions necessary to comply with legislation following a Data Breach or Network Compromise;
- (b) the cost of notifying individuals of a Data Breach who are required to be notified pursuant to any legislation;
- (c) the costs of performing computer forensics to determine the existence, cause, and scope of a Network Compromise or Data Breach;
- (d) the cost of voluntarily notifying individuals of a Data Breach who may not be required to be notified under the applicable legislation;
- (e) the cost of operating a call centre to manage inquiries from individuals affected by the Data Breach;
- (f) the cost of providing credit or identity monitoring and identity protection for those individuals whose Personal Data was or may have been affected by the Data Breach or Network Compromise;
- (g) the fees of a public relations or crisis communications firm solely in order to minimise harm to Your reputation.

72-hour excess waiver: If You notify us within 72 hours of your first awareness of any actual or reasonable suspected Data Breach, the Excess will not apply against any Losses suffered as a result of the Data Breach. This waiver does not apply to any Time Excess.

- **Emergency Response Costs**

We will reimburse you for such expense in respect of emergency payments where it has not been practicable to seek our prior written consent up to 10% of the limit of liability stated in the schedule.



- **Extortion Demands**

Sums paid in response to an extortion demand made against you during the period of insurance, by a third party which has committed or credibly threatens to commit a Network Compromise or a Data Breach, provided that prior to the delivery or transfer of funds, you, after receiving such threat:

- (a) report the extortionist's demand to the police or local law enforcement authorities; and
- (b) had a reasonable belief that such threat was credible, could cause you Loss, and was technologically feasible at the time made.

- **Regulatory Investigations**

Defence costs and insurable fines or insurable civil monetary penalties imposed by a governmental or regulatory authority for a data breach arising from a regulatory investigation.

- **Business Interruption and Increased Cost of Working**

Loss of profit and/or operational expenses, and reasonable costs incurred in addition to normal operational expenses during the period or restoration directly caused by a network compromise. The period of restoration will not in any event exceed ninety (90) days.

- **Loss of Electronic Data**

- (a) costs of replacing, updating or restoring your electronic data which has been destroyed, lost, damaged, or altered during a network compromise from backups, but only up to the level which existed prior to the network compromise;
- (b) costs incurred in remedying the issue which allowed your electronic data to be destroyed, lost, damaged, or altered during a network compromise.

Provides cover for Third Party Losses:

- **Multimedia Internet Liability**

Claims made against you during the period of insurance arising out of the performance of media activities performed by you or your sub-contractors, where the Claim is for:

- (a) negligence or breach of duty to use reasonable skill and care; or
- (b) negligent misrepresentation or negligent misstatement; or
- (c) libel, slander, defamation, product disparagement or trade libel (malicious falsehood); or
- (d) infringement of copyright, or domain name, or the dilution or infringement of any trademark, service mark, service name or trade name; or
- (e) plagiarism or piracy; or
- (f) breach of confidence or misuse of information.



- **Security and Privacy Liability**

Claims, first made in writing against you during the period of insurance, arising out of a privacy and security breach wrongful act by you or your sub-contractors. Privacy and Security Breach Wrongful Act means:

- (a) failure to reasonably protect Personal Data or Confidential Business Information;
- (b) violation of any law, statute, regulation governing the authenticity, availability, confidentiality, storage, control, disclosure, or use of Personal Data;
- (c) violation of a Data Breach Reporting Requirement;
- (d) negligence resulting in a failure to prevent a Network Compromise that results in:
 - (i) the ability of an unauthorised third party user to gain access to Your Computer System;
 - (ii) the malicious addition, alteration, copy, destruction, deletion, disclosure, damage, removal or theft of data residing on Your Computer System;
 - (iii) a Denial of Service attack emanating from Your Computer System which damages, destroys third party hardware, computer programs or Electronic Data residing on a third party's network; or
 - (iv) the transmission of Malware from Your Computer System to a third party.

Provides cover for Ransomware Event Loss: Loss, Loss of Profit, Extortion Demand, Regulatory Fine, Operational Expenses, Defence Costs, or other costs, fees or expenses for, arising out of, in connection with, or in any way involving a Ransomware Event.

Optional endorsement for Cyber Crime providing coverage up to a Sub-Limit of Liability for Social Engineering Financial Fraud Loss, Funds Transfer Fraud Loss or Invoice Manipulation Loss:

- (a) Social Engineering Financial Fraud Event means the transfer of money or securities by you to an account outside your control pursuant to instructions made by a person purporting to be an authorised employee, outsourced provider, vendor or customer of yours, when such instructions prove to have been fraudulent and issued by a person who is not an authorised employee, outsourced provider, or customer of yours.
- (b) Funds Transfer Fraud Event means an unauthorised and fraudulent written, electronic, or telephonic instruction transmitted to a Financial Institution by a third party falsely purporting to be You, directing such Financial Institution to transfer, pay, debit or deliver Money or Securities from Your account, without Your knowledge or consent.
- (c) Invoice Manipulation Fraud Event means the release or distribution of any fraudulent payment instructions to Your client, customer or Vendor as a direct result of a Privacy and Security Breach Wrongful Act in order to mislead or deceive Your client, customer, or Vendor into transferring payment intended for paying an Insured Invoice to another person or entity.



Significant or Unusual Exclusions or Limitations

- Limit of Liability in the aggregate during the period of insurance
- Claims or circumstances known prior to the period of insurance
- Acquisitions and Sales
- Actual or Alleged bodily injury but will not exclude mental anguish or emotional distress caused as a result of a publication breach or data breach
- Liability assumed by you under any contract or agreement, including any guarantees or warranties
- Fraud and dishonesty
- Payment Card Industry (PCI) Fines and Assessments
- Any failure to install and maintain automatically provided updates from the software provider for business critical software
- Wear and tear or failure of any electrical equipment in normal use
- A claim made by you or on your behalf against you
- Legal proceedings brought in a court of law outside the jurisdiction stated in the schedule or brought in a court of law within the jurisdiction stated in the schedule to enforce a judgement or order made in any court of law outside the jurisdiction stated in the schedule
- Any governmental, quasi-governmental or regulatory action or investigation, except with respect the cover offered under the Regulatory Investigation Insuring Clause
- Any actual or alleged physical damage or destruction of any tangible property, including resulting loss of use
- Any Excess and Time Excess applicable to this insurance.
- Extortion Demand and Ransomware Event Loss payment conditions.
- Civil or criminal fines or penalties which are uninsurable under the law governing the policy.

How Do You Cancel?

(a) **Cooling-Off**

If you decide that you do not wish to proceed then you can cancel the policy by notifying your broker or insurance advisor, by email or by telephone within 14 days of either the date you receive your insurance documentation or the start of the policy period whichever is the later. Provided you have not made a claim we will refund the premium and no fee will be charged if the policy is cancelled in the Cooling Off Period.

(b) **Cancellation by Insured**

You may cancel the policy at any time by notifying your broker or insurance advisor. Any return premium due to you will depend on how long the policy has been in force and whether you have made a claim.

(c) **Cancellation by Insurer**

We may cancel the policy, provided there is a valid reason for do so, including for example any failure by you to pay the premium by giving you 14 days' notice in writing. Any return premium due to you will depend on how long the policy has been in force and whether you have made a claim.



How do You Make a Claim?

Claims or circumstances that could give rise to a claim should be notified as follows:

Claims to be notified to in writing:

Angel Risk Management Limited
Marlborough House
Victoria Road South
Chelmsford
Essex
CM1 1LN

Telephone Number: 01245 343630

Email: claims@angelriskmanagement.com

Web: www.angelriskmanagement.com

You will need to quote your Policy number when notifying us.

How Do You Make A Complaint?

We are dedicated to providing a high quality service and we want to ensure that we maintain this at all times.

If you wish to make a complaint you can do so at any time by referring the matter to:

Complaints Department
XL Catlin Services SE, UK Branch
20 Gracechurch Street
London
EC3V 0BG
United Kingdom

Telephone Number: +44 (0)20 7743 8487

Email: axaxlukcomplaints@axaxl.com

XL Catlin Services SE acts on our behalf in the administration of complaints.

If you remain dissatisfied after the complaints department has considered your complaint, or you have not received a final decision within eight (8) weeks, you can refer your complaint to the Financial Ombudsman Service at:

Financial Ombudsman Service
Exchange Tower
London
E14 9SR
United Kingdom

Email: complaint.info@financial-ombudsman.org.uk

Telephone Number: **From within the United Kingdom**

0800 0234 567 calls to this number are free on mobiles and landlines

0300 1239 123 calls to this number costs no more than calls to 01 and 02 numbers



Telephone Number: **From outside the United Kingdom**

+44 (0)20 7964 0500

Fax Number: +44 (0)20 7964 1001

Text Number: 07860 027 586 Call Back Service

The Financial Ombudsman Service can look into most complaints from consumers and small businesses. For more information contact them on the above number or address, or view their website: <https://financial-ombudsman.org.uk>

Financial Services Compensation Scheme (FSCS)

We are covered by the Financial Services Compensation Scheme. The Insured may be entitled to compensation from the Scheme if we are unable to meet our obligations under this contract of insurance. If the Insured were entitled to compensation under the Scheme, the level and extent of the compensation would depend on the nature of this contract of insurance. Further Information about the Scheme is available from the Financial Services Compensation Scheme (10th Floor, Beaufort House, 15 St. Botolph Street, London EC3A 7QU) and on their website: <https://fscs.org.uk>

Fair Processing Notice

This Privacy Notice describes how AXA XL Insurance Company UK Limited (together, “we”, or “us”) collect and use the personal information of insureds, claimants and other parties (“you”) when we are providing our insurance and reinsurance services.

The information provided to us, together with medical and any other information obtained from you or from other parties about you in connection with this policy, will be used by us for the purposes of determining your application, the operation of insurance (which includes the process of underwriting, administration, claims management, analytics relevant to insurance, rehabilitation and customer concerns handling) and fraud prevention and detection. We may be required by law to collect certain personal information about you, or as a consequence of any contractual relationship we have with you. Failure to provide this information may prevent or delay the fulfilment of these obligations.

Information will be shared by us for these purposes with group companies and third party insurers, reinsurers, insurance intermediaries and service providers. Such parties may become data controllers in respect of your personal information. Because we operate as part of a global business, we may transfer your personal information outside the United Kingdom and/or the European Economic Area for these purposes.

You have certain rights regarding your personal information, subject to local law. These include the rights to request access, rectification, erasure, restriction, objection and receipt of your personal information in a usable electronic format and to transmit it to a third party (right to portability).

If you have questions or concerns regarding the way in which your personal information has been used, please contact: dataprivacy@axaxl.com.

We are committed to working with you to obtain a fair resolution of any complaint or concern about privacy. If, however, you believe that we have not been able to assist with your complaint or concern, you have the right to make a complaint to the relevant Data Protection Authority .

For more information about how we process your personal information, please see our full privacy notice at: <http://axaxl.com/privacy-and-cookies>.



axaxl.com

AXA XL Insurance Company UK Limited
20 Gracechurch Street, London, EC3V 0BG, United Kingdom

Telephone: +44 (0)20 7626 0486 Fax: +44 (0)20 7623 9101 **axaxl.com**

AXA XL Insurance Company UK Limited | Registered office: 20 Gracechurch Street, London, EC3V 0BG Registered in England No 1815126
AXA XL Insurance Company UK Limited is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.