CYBER Pro

INSURANCE, RISK MANAGEMENT AND BREACH RESPONSE SERVICES

ASCENT™
UNDERWRITING


has_many :ratings, foreign_
has_many :messages_sent, cl
has_many :messages_received,
accepts_nested_attributes_fo
avatar attachment
adapter options if host
run upon changing host
has_attached_file :avata
5
26
27
28

CYBERPro

CyberPro is a unique and proprietary insurance product based on a modular form concept which combines comprehensive professional services coverage for technology and miscellaneous professionals with a cutting edge cyber liability solution, providing unique non-tangible risk insurance, covering network business interruption, ecommerce trading exposures, crime and protection from media and intellectual property risks. CyberPro also includes loss control education and training; and full post breach crisis management assistance.

CYBERPRO: INSURANCE

CyberPro is suitable for nearly all commercial clients in most industry sectors, and can be adapted to specific needs and requirements. Coverage is provided on a modular basis, with independent insuring agreements so that a policyholder can "pick and choose" their coverage according to requirements.

Please note that this summary is not exhaustive and full terms and conditions can be found in the Policy Wording.

STANDARD KEY COVERAGE

- Security and privacy liability
- Multimedia and intellectual property liability
- Technology services
- Miscellaneous professional services
- Network interruption and recovery
- Event support expenses
- Privacy regulatory defense and penalties
- Network extortion
- Electronic theft, computer fraud & telecommunications fraud
- Social engineering
- Reputational damage
- Coverage extended to cloud providers and external vendors
- Voluntary notification
- Coverage for rogue employees
- Programming and human error
- Worldwide jurisdiction
- Costs to cover Payment Card Industry fines and penalties

ADDITIONAL COVERAGE

Cover may be extended, at an additional premium, to include the following:

- Business interruption and data restoration coverage extension to external vendors
- Notification costs outside of policy limits
- General Liability
- Excess Waiver

MAJOR POLICY EXCLUSIONS

- Wrongful acts committed prior to the retroactive date
- Previously notified claims
- Insured versus Insured
- Fraudulent, dishonest or criminal acts
- Bodily injury and property damage
- OFAC Trade Sanctions
- State or Federal enforcement or investigation
- Terrorist acts
- Patent infringement or misappropriation of trade secrets
- Use of illegal or unlicensed programs
- Unauthorized trading of money, securities, property
- Deceptive, inaccurate, misleading or false advertising

Please note this summary is not exhaustive and all of the Exclusions applied to this Policy can be found in Section VIII – What We Do Not Cover – of the Policy Wording.

CYBERPRO: LOSS CONTROL, EDUCATION AND TRAINING

CyberPro has not only been designed to provide crucial insurance protection but also to respond to constantly evolving risk and regulation that places increasing responsibilities on businesses and how they are required to manage and mitigate Cyber risk.

Ascent provides this service by partnering with relevant, expert professionals who provide up to date advice and information that helps policyholders avoid or minimize breach events and, should such events occur, manage them appropriately and effectively.

CYBERPRO: ELECTRONIC THEFT, COMPUTER FRAUD, TELECOMMUNICATIONS FRAUD AND SOCIAL ENGINEERING

CyberPro provides coverage for monetary loss which you sustain as a result of electronic theft, computer fraud, telecommunications fraud and/or social engineering.

Such coverage relates to certain types of traditional crime such as fraud and theft resulting from a security event, and being perpetrated via misuse of a computer network.

In the instance of a security event, as defined within the policy, coverage under these modules may extend to monetary losses resulting from:

- theft of intangible assets such as data and trade secrets;
- loss or disbursement of money, securities and/or other assets by third parties or by an employee with the intent to defraud;
- creation of fictitious accounts in your name;
- intentional, unauthorised use of your telecommunications system;
- misrepresentation of fact or an intentional, malicious, wilful or fraudulent act undertaken by a third party that misleads an employee into disbursing money, securities and/or other assets.

CYBERPRO: BREACH RESPONSE SERVICES

Depending on the nature of the breach, Ascent will work with a broad range of expert firms and individuals to ensure policyholders receive the specific advice they need to take decisive action, mitigate further loss or exposure and protect their customers:

BREACH RESPONSE

We help our policyholders react swiftly and comprehensively to a privacy breach by utilising experienced breach response teams. In the event of a cyber-related incident, 24x7 contact numbers are available to policyholders so that they can call to seek advice and register the event. Our breach response partner will run immediate triage to gather information about the incident and determine whether follow-up action is required.

Experts may need to attend the client's premises to determine which machines have been affected by the attack and, subject to log information being available, determine how the attackers gained access (in the event of a breach), type of malware/attack used, data accessed/compromised and individuals effected.

A breach counselling service is also available to help evaluate the incident and to determine whether a privacy breach has occurred. In the event of a confirmed breach the team will help assess the severity of the event, explain breach response requirements and share best practices to respond to the situation and mitigate further risk to the policyholder's business.

NOTIFICATION EXPENSES

CyberPro provides cover for reasonable and necessary legal expenses, postage expenses and related advertising expenses, to mitigate damage to a policyholder's brand and/or comply with governmental privacy legislation in the event that personal information has, or could be, compromised. Reimbursement of all such expenses is subject to Ascent's approval.

These expenses will by Ascent's selected service provider(s) dependent on the specific nature of the breach.

In the event of a breach, our partners will guide policyholders through the process of notifying the individuals affected, whether they are their employees, customers, or patients. Our advisers will help policyholders determine the best method of notice (for example, direct mail, email or media disclosure) and select the most appropriate supplier to help them remain compliant and record their actions so that they meet or exceed federal, state and regional requirements. Our suppliers may also provide the following services if relevant to policyholders:

(1) Provision of notification letter template(s) and/or service enrolment documents;

(2) Management, handling, printing and mailing of letters;

(3) Ensure that policyholders customer information is up to date by analysing their customer address database against multiple national databases

(4) Identify incorrect contact information and resolve; or establish alternative notification methods to ensure that as many of the policyholders customers as possible are notified;

(5) Return mail handling, reporting and additional address changing. Printing and mailing of notification letters for returned mail when new addresses are available;

(6) Advertising Services.

FORENSIC AUDITING

Under the CyberPro Network Interruption and Recovery module, cover is provided for the costs of hiring appropriate forensic auditors to review all details relating to a breach and to determine the cause and extent of any theft or unauthorized disclosure of information. This may involve digital and network investigations of hacking incidents, lost and stolen property, cyber extortion, database fraud, offensive communication, and other risks.

Through appropriate forensic investigation the existence, cause and impact of the event may be established, together with the extent to which there may have been unauthorized access or disclosure. All necessary steps to prevent future breaches can also be identified. Ascent's vendors are renowned world-wide for their forensic auditing expertise which is regularly demonstrated in high profile cases. They are experts in network and digital investigations regularly investigating hacking incidents, data and intellectual property theft. Their work also covers cyber extortion, database fraud, cyber defacement and harassment, other offensive digital communications and investigation into other online risks.

We will identify appropriate expert providers to investigate all events including where PCI compliance and approval is required.

SUPPORT, CREDIT AND IDENTITY THEFT SERVICES

To mitigate the impact on policyholder's customers following a compromise or potential compromise of personal information, it may be necessary to deploy certain identity and/or credit management and monitoring services. This is to ensure compliance with certain federal, state and regional requirements and/or provide additional protection and security to affected individuals. These services may include:

(1) Credit file review and report translation, interpreting policyholder's customer credit files and reports and helping them understand the data.

(2) Activation of fraud alerts, to notify potential creditors or lenders to individuals/ entities that may be victims of identity theft.

(3) Monitoring policyholder's customer credit and/or personal data, which may include but is not limited to, multiple bureau credit reporting or monitoring, court records monitoring, change of address monitoring, social security number tracing, payday monitoring and/or cyber monitoring.

(4) Promptly alerting individuals of changes detected through monitoring services, such as new credit applications, new financial accounts, credit enquiries or loans.

(5) Provide individuals with access to electronic education and alerts via email.

(6) Assistance in creating a customer affidavit in the event of fraud.

(7) Dedicated fraud specialists working to gather evidence and help creditors reduce damages and resolve identity theft events. This includes follow up to include tracking of activity and steps taken to resolve the issue.

(8) Systematic notification to any relevant government and private agencies

(9) Assistance with credit file freezes

(10) In the event an affected victim is the subject of a complex identity theft or financial fraud scheme, further investigation and action that goes beyond routine remediation activities may be necessary.

Where sensitive personal information has been harvested as part of an incident Kroll, through their partnership with the CIFAS not for profit organisation can arrange a credit monitoring service and in the event that an individual's credit ratings are adversely affected by the use of stolen information, work with them to restore their credit rating to pre-incident levels.

Full details of the CIFAS service can be found at **https://www.cifas.org.uk/**

CALL HANDLING SERVICES

These services will be provided by one of our preferred partners in consultation with policyholders depending on the specific requirements and nature of the breach. This will provide policyholders customers with a point of contact to obtain information relating to the breach, how it could potentially affect them and pre-agreed related information. Depending on the specific breach and the providers selected to handle it, these services may include;

(1) Working with policyholders towards scripted responses via FAQs from customer service representatives to affected parties, including information regarding the breach. For matters not addressed within the pre-approved FAQs, queries may be redirected to policyholder. Experienced fraud specialists can answer questions about the notification letter, calm fears and provide pre-approved remediation services such as placing fraud alerts or enrolling breach victims in credit monitoring.

(1) Calls answered in line with established service levels

(2) Toll-free access for breach notification recipients

(3) Unlimited one-on-one access to a dedicated fraud specialist

(4) Identification of groups that may need special call handling (i.e., the elderly, minors, foreign language, etc.)

(5) Reporting capabilities, which may include number of calls received, duration of the calls, calls abandoned, top 10 most frequently asked questions, type of information requested, number of individuals with a true identity theft, type of identity theft and resolution assistance provided.

EVENT MANAGEMENT SERVICES

Where applicable, and if policyholders reasonably consider that they need to avert or mitigate damage to their brand following a covered event, reasonable and necessary fees for hiring a public relations consultant will be covered subject to our agreement.

We will work with policyholders to appoint a public relations consultant to interact with the public and media and protect their company's reputation after an incident. In many cases we will consider hiring a local firm or one that policyholders have worked with previously, subject to the right experience and expertise.

Ascent has a working relationship with the following well known firms;

- Davidson Ryan Dore
- Bell Yard Communications
- CNC Communications

LEGAL SERVICES

The law firm DAC Beachcroft will be advising you on all your technology and cyber issues. DAC Beachcroft draw on a unique resource of dedicated technology, privacy and insurance experts who are market leaders in the sector. Key services across the UK, EU and beyond include;

(1) Integrated and co-ordinated cyber protection service, in partnership with leading threat monitoring, IT forensics, crisis communication and burst capacity experts.

(2) Dealing with regulatory notifications and investigations in the UK and EU in the event of a data breach, minimizing exposure to fines and penalties.

(3) Defending mass and test case privacy claims.

(4) Forensic co-ordination and asset tracing against fraud and extortion events, including liaison with enforcement and criminal agencies.

(5) Data protection and privacy compliance including data protection audits, security breaches and notification requirements, handling of complaints to the regulator regarding misuse of personal data, dealing with investigations by the ICO, dealing with complex subject access and freedom of information requests.

(6) Managing claims against 3rd party suppliers in respect of network and business interruption claims.

(7) Protection of IP including commercial secrets, copyright, trademarks, design rights and patents.

(8) E-commerce , m-commerce and PCI issues.

(9) Managing contract disputes that arise in large IT projects including infrastructure, hardware refresh, big-data & cloudbased technologies.

(10) Dealing with PR, defamation, marketing and social media claims and acting in website take-downs.

CANCELLATION

This Policy may be cancelled by either you or us giving notice in writing to your Broker. If you cancel the policy a 30% minimum earned premium shall be applicable with the remaining unearned premium calculated on a pro-rata basis. If we cancel the policy a pro-rata return premium shall be returned. We shall only cancel the policy for non-payment of premium or material misrepresentation with regard to any claim notified under a policy.

This insurance has a cooling off period of 14 days of receiving the policy documents or of the start or renewal date of the policy (whichever is later), should you cancel your policy within this time, you are entitled to a full refund, subject to no claims being made. Please note the preceding sentence only applies to policyholders that meet these eligibility criteria: annual turnover less than Euro 2 million and not more than 10 employees. For cancellation outside of the statutory cooling off period of 14 days, you can cancel this insurance at any time by writing (by e-mail, fax or letter) to your broker.

CLAIMS

In the event of any situation or happening that may give rise to a claim, immediate notice must be given in writing to your Broker. For the full claims procedure, please refer to the Policy Wording.

COMPLAINTS

It is always our intention to provide a first class standard of service. However, if you have any cause for complaint or you wish to make any inquiry regarding this Insurance you should, in the first instance, contact the Insurance Broker or Agent or other intermediary who arranged this Insurance for you.

You can also contact us directly at complaints@ascentunderwriting.com or write to us at:

ASCENT UNDERWRITING LLP
10-12 Eastcheap
London EC3M 1AJ
United Kingdom

If your complaint cannot be resolved by the Complaints Department within two weeks, or if you have not received a response within two weeks you are entitled to refer the matter to Lloyd's. Lloyd's will then conduct a full investigation of your complaint and provide you with a written final response.

Lloyd's contact details are:
COMPLAINTS
Fidentia House
Walter Burke Way
Chatham Maritime
Chatham
Kent ME4 4RN

Telephone: +44 (0) 20 7327 5693
Fax: +44 (0) 20 7327 5225

Email: complaints@lloyds.com

Details of Lloyd's complaints procedures are set out in a leaflet "Your Complaint – How We Can Help" available at **www.lloyds.com/complaints** and are also available from the above address.

If you remain dissatisfied after Lloyd's has considered your complaint, or if you have not received a written final response within eight weeks from the date Ascent received your complaint, you may be entitled to refer your complaint to the Financial Ombudsman Service who will independently consider your complaint free of charge. Their contact details are:

THE FINANCIAL OMBUDSMAN SERVICE
Exchange Tower
London E14 9SR

Telephone: (Fixed): 0800 0234567
Tel (Mobile): 0300 1239123
Tel (Outside UK): +44 (0) 20 7964 0500
Fax: +44 (0)20 7964 1001

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

Please note:

You must refer your complaint to the Financial Ombudsman Service within six months of the date of our final response.

The Financial Ombudsman Service will normally only consider a complaint from private individuals or from a business that has an annual turnover of less than 2 million Euros and fewer than 10 employees.

Financial Services Compensation Scheme

Lloyd's insurers are covered by the Financial Services Compensation Scheme. You may be entitled to compensation from the Scheme if a Lloyd's insurer is unable to meet its obligations under this policy. If you are entitled to compensation under the Scheme the level and the extent of the compensation would depend on the type of business and the circumstances of the claim.

Further information is available from the FSCS.
Financial Services Compensation Scheme at:
10th Floor, Beaufort House,
15 St. Botolph Street,
London EC3A 7QU.

Website: www.fscs.org.uk

ABOUT US

ASCENT™
UNDERWRITING

Ascent is a specialist Managing General Agent underwriting on behalf of a number of Lloyd's Syndicates. We provide innovative insurance solutions either face to face or via our proprietary electronic underwriting platform, and commit to offering an excellent and efficient level of service to our broking partners.

Our team have an in depth level of experience and expertise in our markets, which is reflected within our cutting edge market leading insurance products. We have the ability to offer both off the shelf solutions, and bespoke policies which can be finely tailored to the needs of a specific client.

Ascent believes that all insurance products should be complemented by value added solutions and for this reason we partner with market leading professionals, including risk assessors, forensic experts, and proactive claims management companies that assist our clients in making informed choices and ensure the claims process is smooth and efficient.

ABOUT LLOYD'S

Lloyd's is the world's specialist insurance and reinsurance market. With expertise earned over centuries, Lloyd's is the foundation of the insurance industry and the future of it. Led by expert underwriters and brokers who cover more than 200 territories, the Lloyd's market develops the essential, complex and critical insurance needed to underwrite human progress. Backed by diverse global capital and excellent financial ratings, Lloyd's works with a global network to grow the insured world – building resilience for businesses and local communities and strengthening economic growth around the world.

Every day, more than 50 leading insurance companies, over 200 registered Lloyd's brokers and a global network of over 3,800 Coverholder office locations operate in and bring business to the Lloyd's market.

- £65bn claims paid by Lloyd's in the previous 5 years
- £30bn in gross written premiums in 2016
- 99 specialist syndicates
- 258 brokers
- 3,859 coverholder offices globally

FINANCIAL STRENGTH

Standard & Poor	A+
Fitch	AA-
A.M. Best	A

www.ascentunderwriting.com

ASCENT UNDERWRITING LLP
10-12 Eastcheap, London EC3M 1AJ

T +44 (0) 203 642 8250
F +44 (0) 203 642 8259
E info@ascentunderwriting.com