ASCENT™
UNDERWRITING

CyberPro: Insurance, Risk Management and Breach Response Services

CyberPro is a unique and proprietary insurance product which provides a cutting edge cyber liability solution, and a 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 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 policy holder can "pick and choose" their coverage according to requirements.

Standard key coverage

- Liability coverage extended to cloud providers and external vendors
- Voluntary notification
- Reputational harm
- Crisis management and brand reestablishment
- Most favourable venue language
- 70/30 hammer clause
- Computer crime, electronic theft & telecommunications fraud
- Forensic costs up to the full policy limit
- Programming and human error
- Social engineering coverage
- Pre and post breach risk management services
- Cyber terrorism
- Full Prior Acts

Additional coverage

- Costs to cover Payment Card Industry fines and penalties
- Business interruption and data restoration coverage extension to external vendors
- Notification costs outside of policy limits
- Media coverage extended to physical products
- Contingent bodily injury/property damage

CyberPro Coverage modules

- **Security and privacy liability** provides coverage for an Insured's failure to protect private or confidential information and associated legal liability.
- **Multimedia and intellectual property liability** provides coverage for an insured's liability arising from advertising and intellectual property risks.
- **Network interruption and recovery** provides coverage for a company's own losses and rectification costs from network interruption or following a security breach.
- **Event support expenses** provides coverage for the costs of averting or mitigating public relations damage following a network event, including notification, and the offering of a credit monitoring service to individuals whose personal information may have been compromised.
- **Privacy regulatory defense and penalties** provides coverage for an organization defending itself in the event of a regulatory action following a privacy breach or breach of privacy regulations.
- **Electronic theft, computer fraud & telecommunications fraud** provides coverage for loss of an insured's money or asset arising from network security breach.
- **Network extortion** provides coverage to pay for an extortion threat against the insured's network.
- **Social engineering fraud** provides coverage for loss of money or asset arising from phishing or other electronic scams.
- **Reputational damage** provides coverage for business income loss arising from loss of a services contract and reduction in brand value following a network event.

CyberPro

CyberPro: Loss control, education and training

CyberPro has not only been designed to provide crucial insurance protection but also to respond to constantly evolving regulation and legislation 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.

On-line Learning and Resources

Ascent has partnered with the leading breach response company CyberScout and their employees on the key areas of data risk management. The CyberScout Learning Management System (LMS) is an online training program that equips policyholders with the basic knowledge they need to mitigate and manage risk and keeps them informed of the latest legal, regulatory developments affecting their business.

CYBERSCOUT™

Formerly IDT911

CyberScout eLearning tool offers:

- Three separate learning modules lasting from 25-60 minutes.
- Topics on Data Security and Privacy 101; Data Risk and Privacy Management; and Data Breach Forensics, Liability and Remediation.
- Material relevant to small and medium-sized businesses perceived to have low to high-risk exposure, and their employees and brokers.
- Dynamic assessments that test users with new questions every time they undertake one of the eLearning modules.
- Printed certificates upon course completion.
- Access to breach specialists to fully prepare and equip policyholders to meet regulatory response deadlines, government rules and other key steps required to protect their business from potential fines and lawsuits and to preserve their reputation.

Breach Response Web Portal

The Breach Response website enables users to:

- Prepare for the worst by sharing data protection best practice via educational tips, breach scenarios and a risk assessment calculator.
- Review privacy laws and guidelines for each state and province outlined in a quick summary guide.
- Develop an incident response plan that walks users through breach discovery and assessment, internal and external communication protocols and steps to establish a process for handling a breach to minimize impact.
- Access the Knowledge Center which provides informative and up to date educational content on relevant topics, industry trends and regulatory change via news articles, white papers and blog posts.

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 data privacy breach by using the CyberScout Breach response team. This team of experts assists with outlining a clear response strategy and supports our policyholders following a data loss incident.

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 may be handled by CyberScout or a number of other service providers dependent on the specific nature of the breach.

In the event of a breach, our partners will to 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 needs:

Breach Response Services continued...

(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 analyzing their customer address database against multiple national databases (such as Coding Accuracy Account System (CAAS), National Change of Address (NCOA), and Locatable Address Conversion System (LACS);

(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.

In conjunction with CyberScout, we will identify appropriate expert providers to investigate an event and where they need to be PCI approved, we would work with providers selected from the following list:
https://www.pcisecuritystandards.org/approved_companies_providers/pfi_companies.php

Where there is no PCI approval required, we will select providers we have worked with before and whom we know provide the necessary expertise and service.

These providers including the following;

Secureworks (Dell):
http://www.secureworks.com/incident-response

Trustwave:
https://www.trustwave.com/home

Security Metrics:
https://www.securitymetrics.com

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 (including but not limited to Social Security Administration, Internal Revenue Service, Department of Motor Vehicles, Federal Trade Commission, Attorney General Office, Financial Institutions, Check Systems, Collection Agencies)

(9) Assistance with credit file freezes (in States where it is available and in situations where it is warranted)

(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.

All of the above services can be provided through CyberScout and/or other agreed providers, as required by the nature and details of the breach.

Breach Response Services continued...

Call Handling Services

These services may be provided by CyberScout or providers selected 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.

(2) Calls answered in line with established service levels

(3) Toll-free access for breach notification recipients

(4) Support for English, Spanish and other languages

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

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

(7) 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.

For policyholders' larger customers with international operations we have worked with Fleishman Hillard.

Legal Services

In the event that legal advice is required we have worked with many of the best privacy lawyers in their capacity as breach coaches and defence counsel; providing advice on the best course of action to take and how to comply with the applicable Breach Notice Laws and other credit card related regulations. Our experience shows that it is imperative to have the right experts and professionals acting as breach coaches and defence counsel and that they have a successful track record in handling matters with state AGs. We work with a number of expert lawyers, some of which are listed below.

USA

Theodore J. Kobus III
Baker Hostetler
45 Rockefeller Plaza
11th Floor
New York, NY 10111
tkobus@bakerlaw.com

Melissa K. Ventrone, Partner
Wilson Elser Moskowitz Edelman
& Dicker
55 West Monroe Street
Suite 3800
Chicago, IL 60603
312-821-6105

David Navetta, Partner
Info Law Group
1117 S. Clarkson Street
Denver, CO 80210
303-325-3528

Linn F. Freedman, Partner
Nixon Peabody
One Citizens Plaza
Suite 500
Providence, RI 02903
P: 401-454-1108

Joseph J. Lazzarotti, Esq.
Jackson Lewis LLP
220 Headquarters Plaza
East Tower, 7th Floor
Morristown, NJ 07960
973-538-6890

Todd Carlisle
Attorney at Law
Sirote & Permutt, PC
2311 Highland Avenue South
Birmingham, AL 35205
P: (205) 930-5154

Canada

Eric Dolden
Dolden Wallace Folick LLP
888 Dunsmuir St
10thFloor
Vancouver, BC V6C3K4
T: 604-891-0350

Andrea York
Blake, Cassels & Graydon LLP
199 Bay Street
Suite 4000,
Commerce Court
West Toronto, ON M5L1A9

CyberPro

CyberPro: Key Contacts

In the event of a breach policyholders should check their policy or certificate and then, depending on the nature of the claim, or in the event of a privacy breach, they will need to contact the Counsel specified in their policy and/or seek advice from the following:

CyberScout Breach Hotline open 24/7:
Call: 1-800-493-0943
Email: Breach@CyberScout.com
Attn: Mr Eduard Goodman

ASCENT™
UNDERWRITING

About Us

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.

CYBERSCOUT™

Formerly IDT911

About CyberScout

CyberScout is North America's premier identity management and data risk management services provider. Since 2003 they have been leading the charge against hackers, thieves and even simple human error. They provide unrivalled solutions that deliver valuable prevention education, proactive protection services and swift and appropriate incident remediation for more than 770,000 businesses and 17.5 million households.

Their services are provided through various client partners, including Ascent, insurance carriers, major credit unions, banks and numerous Fortune 500 companies.

CyberScout's longstanding reputation, industry expertise and scalable approach offer businesses and their customers a trusted ally for:

- Identity Management
- Breach Education, Preparation, Response and Remediation
- Fraud, Credit and Reputation Monitoring
- Cyber Security and Data Privacy Consulting

Through their consulting operations, CyberScout's experienced professionals help businesses identify their most valuable information assets and the specific vulnerabilities that put their business at risk. Their team can immediately enhance a business' security posture in critical areas to help them comply with privacy regulations, improve the probability of preventing a data breach.

Ascent Underwriting LLP
10-12 Eastcheap, London EC3M 1AJ
www.ascentunderwriting.com

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