Cyber Insurance

We offer a range of insurance products and risk management solutions developed in response to the demands and expectations of the business sector, from minor risks to major exposures.

Our emphasis is on providing:

- professional insurance services
- comprehensive insurance programs tailored to your individual needs
- responsive and proactive claims service
- an extremely competitive price structure.

Our in-depth understanding of credit insurance comes from extensive experience in the worldwide market since 1990. Over the years we have earned a reputation for integrity, creative solutions and outstanding service. For you that means real benefits, personal attention and fast claim settlements.

Cyber Insurance

Cyber-attacks or data breaches can take many forms, from deliberate attacks to technology issues or simple negligence. As modern business is reliant on computer systems and networks, a breach of data or a shut-down of service can have a major impact on your business with many small businesses unable to operate afterwards.

All businesses are vulnerable to cyber-attacks of all kinds and it can be very costly. Aside from the cost of notifying your customers, you may also face costs for public relations, credit monitoring, investigations response and compliance related activity, compensation for affected customers and engaging experts.

With the new Privacy legislation introduced in March 2014, and increased publicity around cyber-attacks, has come a heightened awareness of privacy and cyber exposures. The numbers are alarming with more than 20% of Australian businesses experiencing cyber-crime, and 40% of all attacks directed at SME's.

Cyber Insurance policies can offer cover in the following areas:

- **Third Party Claims** - covers the Insured's liability to third parties from a failure to keep data secure, such as claims for compensation by third parties, investigations, defence costs and fines and penalties from breaching the Privacy Act.

- **First Party Costs** - reimburses the Insured for the costs they would incur to respond to a breach, such as IT Forensic Costs, Credit Monitoring Costs, Public Relations Expenses and Cyber Extortion Costs (including ransom payments to hackers).

- **Business Interruption** - this section provides reimbursement for the Insured's loss of profits resulting from the breach, as well as any additional necessary expenses it may need to incur to continue business as usual

Most of these costs aren't covered by normal business insurance, which is why it is important to speak to us to make sure you are covered in case of a breach or attack.

Let us work with you to develop an insurance program tailored to your specific requirements.

A.I.S. Insurance Brokers Pty Ltd
137 Moray Street
South Melbourne, VIC 3205
Phone: +61 3 8699 8888
Toll free: 1300 300 715
Fax: +61 3 8699 8899
E-mail: insure@aisinsurance.com.au
www.aisinsurance.com.au

Cyber Insurance

Emerging Threat of Cyber Crime

- 700,000 businesses have been impacted by a cyber incident
- 280 days is the average time a hacker is inside a company's IT system before detection
- 60% of all targeted attacks were small to medium sized businesses
- $276,232 is the average cost of a cyber incident
- Companies with 1-250 staff were the most likely target
- The average time to resolve a cyber attack :- 21 days or 51 days if malicous insider / employee is involved
- 72% of cyber tactics involve phishing emails with 23% of recipients opening the email and 17% clicking on attachments
- 50% of Cyber Costs are caused by web based attacks
- 53% of all Cyber costs ($146,451 on average) are spent on detection and recovery

Source – 2017 CGU Cyber Insurance statistics

Cyber Insurance

Cyber Risks Insurance - Claims Examples

One of the best ways to understand your exposure and how this type of insurance can assist in the management of your risks is to look at some of the recent circumstances which may be relevant to you.

Scenario one:	
Profile	Travel agency with four locations, $10M turnover and 30 staff
Background:	The Insured experienced three separate data breaches over a three-year period in which hackers gained access to the Company's computer system. Over 250,000 individuals' credit card information and passport details were compromised.
Policy Response:	Privacy Protection, Breach Costs
Outcome:	$1,750,000 paid for the forensic and legal costs in defending the investigation brought by the regulator and the cost of notifying the affected individuals including providing credit monitoring services.
Scenario two:	
Profile:	Charity with turnover of $18M and 80 staff
Background:	The Insured was targeted with a denial of service attack (floods a targeted system with incoming web traffic until it is virtually crippled) in the last few days of a fundraising campaign. People were unable to make donations for a day while the website was being fixed.
Policy Response:	Cyber Business Interruption, Hacker Damage
Outcome:	$1,500,000 paid for the lost donations and rectifying the damage to the Insured's website.
Scenario three:	
Profile:	Online Retailer with turnover of $5M and 15 staff
Background:	The Insured's website was defaced and included a link to a competing retailer's website when hackers gained access to personal information of their customers and overtook their website.
Policy Response:	Cyber Business Interruption, Hacker Damage, Privacy Protection, Breach Costs
Outcome:	$800,000 was paid for loss of income, cost to repair the website as a result of the hack, defense costs for regulatory actions by the Privacy Commissioner, and costs of notifying the affected individuals including providing credit monitoring services.
Scenario four:	
Profile:	Legal Firm with turnover of $2M and 8 staff
Background:	The Insured's server and client records were locked by Ransomware software. The Insured was only able to get the files released after paying a ransom of $50,000 to hackers.
Policy Response:	Cyber Business Interruption, Cyber Extortion, Hacker Damage
Outcome:	$150,000 paid for the loss of income, the random demand including consultants' costs to advise on handling and negotiation of the ransom, and costs to restore the network as the hackers refused to release the files despite random payment.