Delphic | INSURANCE SERVICES

Cyber Liability Insurance

Private Enterprise <$50m

IMPORTANT NOTICES
For your protection under legislation, we are required to inform you of your duty of disclosure and draw your attention to the following important information.

INTRODUCTION
The Insurance Contracts Act 1984 requires insurance companies to provide certain information to people intending to insure with them. The information concerns the duty of disclosure of an intending Insured and the effect of particular types of clauses in a proposed insurance policy. Where an Insurance Broker is involved in the transaction, the information is to be provided by the broker. The Insurance (Agents and Brokers) Act 1984 also requires us to inform you about some other matters where they are relevant to particular policies.

WHAT INFORMATION DOES AN INSURANCE COMPANY/BROKER HAVE TO GIVE YOU?
In general terms, the kind of information, which an insurance company/broker must give you, is as follows:

YOUR DUTY OF DISCLOSURE
Before you enter into a contract of general insurance with an Insurer, you have a duty, under the Insurance Contracts Act 1984, to disclose to the Insurer every matter that you know, or could reasonably be expected to know, that is relevant to the Insurer's decision whether to accept the risk of the insurance, and if so on what terms.

You have the same duty to disclose those matters to the Insurer before you renew, extend, vary or reinstate a contract of general insurance.

Your duty, however, does not require disclosure of matter:

- that diminishes the risk to be undertaken by the Insurer,
- that is of common knowledge,
- that your Insurer knows or, in the ordinary course of his business, ought to know,
- as to which compliance with your duty is waived by the Insurer.

NON-DISCLOSURE
If you fail to comply with your duty of disclosure, the Insurer may be entitled to reduce his liability under the contract in respect of a claim or may cancel the contract.

If your non-disclosure is fraudulent, the Insurer may also have the option of voiding the contract from its beginning.

CLAIMS MADE INSURANCE
Your attention is drawn to the fact that if the Professional Indemnity section of this policy is selected, the cover will be placed on a "claims made" basis which means that claims first advised to you (or made against you) and reported to your insurer during the Period of Insurance are recoverable irrespective of when the incident causing the claim occurred, subject to the provisions of any clause relating to a "retroactive date".

You should also note that, in terms of the provisions of Section 40(3) of the Insurance Contracts Act 1984, where you give notice in writing to the Insurer of facts that might give rise to a claim against you as soon as is reasonably practicable after you become aware of those facts (but before the insurance cover provided by the contract expires) then the Insurer is not relieved of liability under the contract in respect of the claim, when made, by reason only that it was made after the expiration of the Period of Insurance cover provided by the contract.

RETROACTIVE LIABILITY
The policy may be limited by a retroactive date stated in the schedule. The policy does not provide cover in relation to any claim arising from any actual or alleged act, error, omission or conduct that occurs before the commencement of the policy, unless retroactive liability cover is extended by Underwriters.

LIABILITY ASSUMED UNDER AGREEMENT
Cover provided by this form of liability insurance does not cover liability which you have agreed to accept unless you would have been so liable in the absence of such agreement.

UTMOST GOOD FAITH
In accordance with Section 13 of the Insurance Contracts Act 1984 (Cth), the policy of insurance is based on utmost good faith requiring Underwriter(s) and the proposer / insured(s) to act towards each other with the utmost good faith in respect of any matter relating to the insurance contract.

PRIVACY NOTICE
Please refer to our privacy policy for further details, it is available on our website, www.delphicinsurance.com.au.

Please note that your duty applies also when you seek to renew, extend, alter or reinstate a policy.

Alternatively, if you have any query about whether information needs to be disclosed, please contact our office.

Delphic

Cyber private enterprise

Insurance application form

This application form is for companies with revenues of less than $50m who are looking for cyber insurance limits of $5m or below. If you would like further information about the cover available or assistance with completing this form then please contact our office.

Basic company details

Please complete the following details for the entire company or group (including all subsidiaries) that is applying for the insurance policy:

Company Name: Primary Industry Sector:

Primary Address (Address, State, Postcode, Country):

Description of Business Activites:

Website Address:

Date Established (DD/MM/YYYY):

Are you GST registered? □ Yes □ No *If "yes", please state your ABN:*

Last Complete Financial Year Revenue: $ Revenue From US Sales (%):

Primary contact details

Please provide details for the primary contact for this insurance policy:

Contact Name: Position:

Email Address: Telephone Number:

Coverage required

Please indicate which limit options you would like to recieve a quotation for (if cover is not required for a particular area please leave blank):

Cyber Incident Response:	□ $250k	□ $500k	□ $1m	□ $2m	□ $5m	□ Other $	
Cyber & Privacy Liability:	□ $250k	□ $500k	□ $1m	□ $2m	□ $5m	□ Other $	
System Damage & Business Interruption:	□ $250k	□ $500k	□ $1m	□ $2m	□ $5m	□ Other $	
Cyber Crime:	□ $100k	□ $250k	□ $1m	□ Other $			

Previous cyber incidents

Please tick all the boxes below that relate to any cyber incident that you have experienced in the last three years(there is no need to highlight events that were successfully blocked by security measures):

□ Cyber Crime	□ Cyber Extortion	□ Data Loss	□ Denial of Service Attack	□ IP Infringement
□ Malware Infection	□ Privacy Breach	□ Ransomware	□ Other (please specify)	

If you ticked any of the boxes above, did the incident(s) have a direct financial impact upon your business of more than $10,000? □ Yes □ No

If yes, please provide more information below, including details of the financial impact and measures taken to prevent the incident from occuring again:

Important Notice

By signing this form you agree that the information provided is both accurate and complete and that you have made all reasonable attempts to ensure this is the case by asking the appropriate people within your business. Insurers will use this information solely for the purposes of providing insurance services and may share your data with third parties in order to do this.

Contact Name: Position:

Signature: Date (DD/MM/YYYY):

Delphic

Cyber private enterprise

Insurance application form

Further information helps us obtain a more complete picture of your company and the security controls you have in place. By completing this additional request for information we may be able to negotiate more favourable premiums on your quote. If you would like further information about the cover available or assistance with completing this form, please contact our office.

Revenue Analysis

Please complete the answers to the questions below. Where you do not have the exact information available please provide the closest approximation and indicate that you have taken this approach.

Please provide the following details for your top 5 clients:

Client name:	Primary Services:	Annual Revenue:

IT resourcing and infrastructure

What was your approximate operational expenditure on IT security in the last financial year (including salaries, annual licenses, consultancy costs, etc.):

What was your approximate capital expenditure on IT security in the last financial year (including hardware, one off software costs, etc.):

Do you anticipate spending more, the same or less in this financial year?

Is your IT infrastructure primarily operated and managed in-house or outsourced?

If it is outsourced, who do you outsource it to?

How many full-time employees do you have in your IT department?

How many of these employees are dedicated to a role in IT security?

Information security governance

Who is responsible for IT security within your organisation (by job title)?

How many years have they been in this position within your company?

Please describe the type, nature and volume of the data stored on your network:

Please describe your data retention policy:

Do you comply with any internationally recognised standards for information governance (if yes, which ones):

Cloud service providers

Please tick all the boxes below that relate to companies or services where you store sensitive data or who you rely upon to provide critical business services:

□ Adobe
□ Amazon Web Services
□ Dropbox
□ Google Cloud
□ IBM
□ Microsoft 365
□ Microsoft Azure
□ Oracle Cloud
□ Rackspace
□ Salesforce
□ SAP
□ Workday
□ Other (please specify):

Cyber security controls

Please confirm that multi-factor authentication is always enabled on all email accounts: □ Yes □ No

Please state which technology you use for remote access to ensure its security:

How often do you patch your operating sytems?

How often do you conduct vulnerability scanning of your network perimeter?

How often do you conduct pentration testing of you network architecture?

Please provide details of the third party providers you use to conduct penetration testing:

Please describe your data back up policy:

Please tick all the boxes below that relate to controls that you currently have implemented within your IT infrastructure (including where provided by a third party).
If you're unsure of what any of these tools are, please refer to the explanations on the final page of this document.

□ Advanced Endpoint Protection
□ Application Whitelisting
□ Asset Inventory
□ Custom Threat Itelligence
□ Database Encryption
□ Data Loss Prevention
□ DDoS Mitigation
□ DMARC
□ DNS Filtering
□ Employee Awareness Training
□ Incident Response Plan
□ Intrusion Detection System
□ Mobile Device Encryption
□ Penetration Tests
□ Perimeter Firewalls
□ Security Info & Event Management
□ Two-factor Authentication
□ Vulnerability Scans
□ Web Application Firewall
□ Web Content Filtering

Please provide the name of the software or service provider that you use for each of the controls highlighted above:

Delphic

Cyber private enterprise

Insurance application form

Important notice

By signing this form you agree that the information provided is both accurate and complete and that you have made all reasonable attempts to ensure this is the case by asking the appropriate people within your business. Insurers will use this information solely for the purposes of providing insurance services and may share your data with third parties in order to do this.

Contact Name:		Postion:	
Signature:		Date (DD/MM/YYYY):	

Cyber security controls explained

Advanced endpoint protection

Software installed on individual computers (endpoints) that uses behavioural and signature based analysis to identify and stop malware infections.

Application whitelisting

A security solution that allows organisations to specify what software is allowed to run on their systems, in order to prevent any nonwhitelisted processes or applications from running.

Asset inventory

A list of all IT hardware and devices an entity owns, operates or manages. Such lists are typically used to assess the data being held and security measures in place on all devices.

Custom threat intelligence

The collection and analysis of data from open source intelligence (OSINT) and dark web sources to provide organisations with intelligence on cyber threats and cyber threat actors pertinent to them.

Database encryption

Where sensitive data is encrypted while it is stored in databases.
If implemented correctly, this can stop malicious actors from being able to read sensitive data if they gain access to a database.

Data loss preventions

Software that can identify if sensitive data is being exfiltrated from a network or computer system.

DDoS mitigation

Hardware or cloud based solutions used to filter out malicious traffic associated with a DDoS attack, while allowing legitimate users to continue to access an entity's website or web-based services.

DMARC

An internet protocol used to combat email spoofing – a technique used by hackers in phishing campaigns.

DNS filtering

A specific technique to block access to known bad IP addresses by users on your network.

Employee awareness

Training programmes designed to increase employees' security awareness. For example, programmes can focus on how to identify potential phishing emails.

Incident response plan

Action plans for dealing with cyber incidents to help guide an organisation's decision-making process and return it to a normal operating state as quickly as possible.

Intrusion detection system

A security solution that monitors activity on computer systems or networks and generates alerts when signs of compromise by malicious actors are detected.

Mobile device encryption

Encryption involves scrambling data using cryptographic techniques

so that it can only be read by someone with a special key. When encryption is enabled, a device's hard drive will be encrypted while the device is locked, with the user's passcode or password acting as the special key.

Penetration tests

Authorised simulated attacks against an organisation to test its cyber security defences. May also be referred to as ethical hacking or red team exercises.

Perimeter firewalls

Hardware solutions used to control and monitor network traffic between two points according to predefined parameters.

Security info & event management (SIEM)

System used to aggregate, correlate and analyse network security information – including messages, logs and alerts – generated by different security solutions across a network.

Two-factor authentication

Where a user authenticates themselves through two different means when remotely logging into a computer system or web based service. Typically a password and a passcode generated by a physical token device or software are used as the two factors.

Vulnerability scans

Automated tests designed to probe computer systems or networks for the presence of known vulnerabilities that would allow malicious actors to gain access to a system.

Web application firewall

Protects web facing servers and the applications they run from intrusion or malicious use by inspecting and blocking harmful requests and malicious internet traffic.

Web content filtering

The filtering of certain web pages or web services that are deemed to pose a potential security threat to an organisation. For example, known malicious websites are typically blocked through some form of web content filtering.