NZI LIABILITY CYBER BASE & ULTRA

INSTANT QUOTE: for Manufacturing, Wholesale, Construction, Transportation, Entertainment, Education, Professionals and Rural with revenue derived from New Zealand/Australia only. Please consult your Broker should your business activities fall outside of this list.

YOUR DUTY OF DISCLOSURE

You must tell us all information you know (or could reasonably be expected to know) which would influence the judgement of a prudent underwriter whether or not to accept your application, and if it is accepted, on what terms and at what cost.

Examples of information you may need to disclose include:

- anything that increases the risk of an insurance claim;
- any criminal convictions in the last 7 years or where imprisoned;
- if another insurer has cancelled or refused to renew insurance, or has imposed special terms;
- any insurance claim you have made in the past.

Examples of information you do not need to disclose include:

- anything that reduces the risk of an insurance claim;
- anything we say you do not need to tell us about;
- anything that is common knowledge;
- anything you have already told us, or that we should be expected to know in the ordinary course of our business.

These examples are a guide only. If you are not sure whether you need to disclose a particular piece of information, please ask.

WHEN IN DOUBT – DISCLOSE. ALL INFORMATION WILL BE TREATED CONFIDENTIALLY.

YOUR DETAILS

Insured (include all entities to be insured)	
Insured Business (include activities of all entities)	

YOUR SELECTION

CYBER BASE

Total Annual Gross Revenue	Limit of Indemnity (Any One Claim/Aggregate)	Please tick option
NZ$0 to NZ$10,000,000	$250,000	❑

CYBER ULTRA

Total Annual Gross Revenue	Limit of Indemnity (Any One Claim/Aggregate)	Please tick option
NZ$0 to <NZ$1,000,000	$500,000	❑
	$1,000,000	❑
	$2,000,000	❑
NZ$1,000,000 to <NZ$5,000,000	$500,000	❑
	$1,000,000	❑
	$2,000,000	❑
NZ$5,000,000 to NZ$10,000,000	$500,000	❑
	$1,000,000	❑
	$2,000,000	❑

NOTE:

- Premiums shown are annual premiums. Premiums are subject to change.
- If you require an indication for a higher revenue or higher limit of indemnity, please refer to your Broker for further advice.
- Coverage summary, sub-limits and excesses are overleaf.

RISK MANAGEMENT

1. When removing data/information from your premises on portable media (e.g. USB, flash memory, disk hard drive or tape), is it encrypted? Yes ❑ No ❑

   This is to prevent the data/information being accessed if the portable media is lost/stolen.

   N.B. If "No", unencrypted portable media exclusion will be applied.

2. Do you regularly update (at least monthly) firewalls and virus protection software in place within your networks? Yes ❑ No ❑

   This is to ensure that security measures are updated to protect against the latest malware/viruses.

   N.B. If "No", we are unable to provide cover.

3. Do you have back-ups stored off-site, and tested at least annually? Yes ❑ No ❑

   In the event of a cyber attack, the business will rely on the back-ups to restore their system. The back-up needs to be tested regularly to ensure the integrity of the data.

   N.B. If "No", we are unable to provide data recovery or business interruption cover.

VENDOR MANAGEMENT

Please identify your critical vendors:

Type of Vendor	Yes	No	Name of Vendor
Cloud / Back-up / Web Hosting	❑	❑	
Internet Service Provider (ISP)	❑	❑	
Business Critical Software Provider	❑	❑	
Data Processors (e.g. payment processing)	❑	❑	
POS Hardware Provider	❑	❑	
Managed Security Services (e.g. firewall, intrusion detection, anti-virus)	❑	❑	

CLAIMS AND CIRCUMSTANCES

Please answer the following questions after enquiry within your organisation.

1. During the past 5 years has any claim been made, or have any circumstances which may give rise to a claim, against any entity or individual to be insured by this insurance been notified to insurers? Yes ❑ No ❑
2. Are there any circumstances not already notified to insurers which may give rise to a claim against any entity or individual to be insured by this insurance? Yes ❑ No ❑
3. Has any principal or staff member ever been subject to disciplinary proceedings, regulatory action, or investigation by any Government, regulatory or administrative agency? Yes ❑ No ❑

If you have answered "Yes" to any of the above questions, please provide full details and refer to your Broker for further advice.

CLAIMS SCENARIOS

1. The business

A South Island panel beating firm.

The Cyber attack

The breach was first detected after a staff member was unable to log into their IT system. After further investigation, they discovered that a number of files were missing.

The Insured immediately took their system offline and informed their broker of the attack. From here several notifications and actions took place:

- The Insured's broker contacted NZI's Cyber Hotline to report the incident.
- Breach coordinators, Cunningham Lindsey, immediately contacted the Insured and reported the notification to NZI.
- NZI engaged Deloitte to investigate the attack and assist in the re-establishment of the Insured's systems.

Deloitte's initial investigation confirmed that the client was the victim of a Ransomware attack and assisted the Insured to identify the backup files required to restore the system that same day.

NZI in conjunction with Cunningham Lindsey let the Insured know what they needed to do to minimise business disruption. Due to the urgency of the matter regular contact was maintained with Cunningham Lindsey throughout the day.

The following morning a temporary PC was set up so that basic business operations could continue and by the next day the Insured's IT systems had been fully restored. NZI also approved the employment of temporary staff to assist the client in manually re-entering any lost data which included a significant number of job quotes.

Deloitte conducted a thorough investigation and made a number of recommendations on how the Insured's IT security could be improved to help avoid further attacks.

Cost of the claim

Costs are ongoing with the overall claim expected to be in the region of $136,000.

2. The business

Nuke-it Appliances (Nuke-it) is a wholesaler of kitchen appliances throughout New Zealand.

The Cyber attack

The client was notified by its web-hosting provider, Hostinator, that its website had been hacked. Hostinator advised the client that they viewed logs and confirmed the website was being used to send spam emails. They suspended the site and instructed the insured to contact a web developer to clean the site.

Nuke-it immediately called Cunningham Lindsey who in turn contacted Deloitte for assistance. Deloitte investigated and found source of the spam was a fairly common malicious file called "list.php" which contains code required to launch the spam attack. Data logs showed that the attack was launched at 6.40am one morning and lasted around 5 hours. The attack was launched from multiple IP addresses indicating that the attacker was operating through a set of "proxy" servers, to mask their identity. Deloitte advised that the website had been unmanaged in regards to security, patches and updates that meant it was vulnerable to attack. Deloitte immediately redirected the original URL to a sister company in order to minimise disruption and potential loss of business.

Deloitte were able to repair the website and have it back online in the same day they received agreement from Nuke-it to do so and continued to perform spot checking of the website content and logs over the following 7 days. In that period they found only regular scanning and basic credential exploitation attempts (i.e. users unsuccessfully trying to login in to interfaces using default credentials) – all of which is common place for a website on shared hosting. They discovered that someone had already commenced trying to exploit a new critical vulnerability by adding an unauthorised administrator account. Fortunately, because Deloitte identified the critical weakness in the software and subsequent breach of it, they were able to swiftly remedy this and did so free of charge.

When handing full control back to Nuke-it, Deloitte also recommended that they ask their IT vendor to update and maintain the site as new patches are released, and to move the site hosting to a comparably priced but improved hosting provider.

Cost of the claim

The total cost amounted to approximately $16,000.

DECLARATION

I / We hereby declare that:

The above statements are true, and I / we have disclosed all material facts and should any information given by me / us alter between the date of this Application form and the inception date of the insurance to which this Application relates I / we shall give immediate notice thereof.

I / We authorise NZI, a business division of IAG New Zealand Limited, to collect or disclose any personal information relating to this insurance to / from any other insurers or the Insurance Claims Register.

I / We also confirm that the undersigned is authorised to act for and on behalf of all persons who may be entitled to indemnity under any policy which may be issued pursuant to this Application form and I / we complete this Application form on their behalf.

To be signed by the Chairman / President / Managing Partner / Managing Director / Principal of the association / partnership / company / practice / business.

Signature: _____

Position: _____

Date: _____

It is important the signatory / signatories to the Declaration is / are fully aware of the scope of this insurance so that all questions can be answered. If in doubt, please contact your insurance broker since non-disclosure may affect an Insured's right of recover under the policy or lead it to being voided.

Cover will be bound on Our receipt of Your advice of acceptance of this quotation.
The terms of this quotation remain valid for 30 days from the date this Declaration was signed, provided that

1. no Claims have arisen, and
2. there have been no changes to the risk proposed for insurance, between the date the Declaration was completed and the proposed date of commencement of insurance.

The proposed Period of Insurance can commence no earlier than the date of Our receipt of Your advice that this quotation is accepted.

PRIVACY ACT STATEMENT

We gather information about you (including your claims history) to consider your application for insurance. Your duty of disclosure requires you to do this. If you refuse to provide the information, we may decline your application or declare this policy unenforceable from the beginning.

This information is held by us and you may access and seek correction of it. It may be passed on to other insurers you deal with, and interested parties.

Your claims history is passed on to, and held by, Insurance Claims Register Ltd. This enables other insurers you deal with to access it, and prevents fraudulent claims.

POLICY COVERAGE, LIMITS AND EXCESSES

Cover	Explanation	Cyber Base	Cyber Ultra	Limit of Indemnity/ Sub-limit	Excess (each & every claim)
Privacy	Loss of personal or corporate information (including employee information). Loss of personal information held by service providers (for example, the Cloud, or internet service providers). Defence costs.	✓	✓	Full Limit of Indemnity	$2,500
System damage	Lost, damaged or destroyed IT systems and IT records/data. Costs of retrieving, repairing, restoring or replacing data, systems or hardware. Costs of external IT forensic or security consultants.	✓	✓	Full Limit of Indemnity	$2,500
Business interruption	Loss of profits due to a cyber event (with no indemnity period restriction).	✗	✓	Full Limit of Indemnity	12 hours
Computer virus transmission and hacking	Liability arising from hacker attacks or viruses. Loss or theft of your data (or data for which you are responsible). Loss by phishing emails or denial of services attacks. Attacks by employees and third parties.	✓	✓	Full Limit of Indemnity	$2,500
Computer Crime	Crime losses, including loss of money or property. Loss of money or property from service providers' system. Loss caused by rogue employee or third party.	✗	✓	$100,000	$2,500
Multimedia liability	Protection against libel, slander or defamation. Cover for infringement of copyright, trademarks and trade names – on all your marketing material (digital or print). Covers your defence costs and third party's costs.	✓	✓	Full Limit of Indemnity	$2,500
Breach of statutory duties relating to e-commerce	Breach of statutory duty from e-Commerce business. Defence costs and compensation.	✗	✓	Full Limit of Indemnity	$2,500
Cyber extortion cover	Payment of ransom, or costs associated with negotiating or mediating due to an extortion attempt. Crisis management costs.	✓	✓	Full Limit of Indemnity	$2,500
Brand and personal protection cover	Public relations consultancy costs to protect your company brand(s) and personal reputations of senior executives.	✗	✓	Full Limit of Indemnity	$2,500
Privacy fines and investigations	Fines and penalties you incur due to a privacy breach. Defence and investigation costs.	✓	✓	Full Limit of Indemnity	$2,500
Privacy breach notification and loss mitigation	Breach costs (for actual or suspected privacy breach), including credit monitoring, identify theft monitoring, data restoration and forensic costs. Legal costs.	✓	✓	Full Limit of Indemnity	$2,500
Free cyber consultation	Free advice from a member of our Cyber expert panel in relation to a cyber issue.	✗	✓	1 hour	No excess applies
Reward expenses	Payment of a reward for information leading to a conviction relating to a hacking attack.	✓	✓	Full Limit of Indemnity	$2,500
Payment card industry fines and penalties	Fines and penalties you incur due to the failure to comply with the Payment Card Industry Data Security Standard.	✗	✓	25% of the Limit of Indemnity	$2,500

Territorial and Jurisdiction Limits

Territory: Worldwide

Jurisdiction: Worldwide excluding USA/Canada

Retroactive Date: Policy Inception

FINANCIAL STRENGTH RATING

NZI is a business division of IAG New Zealand Limited which received a Standard & Poor's (Australia) Pty Ltd financial strength rating of AA-.

This means we have a 'Very Strong' claims paying ability, as you can see in the scale below. As a customer, this is important to you as it's your reassurance that we will be able to pay your claims now and in the future.

The rating scale is:

AAA	(Extremely Strong)	CCC	(Very Weak)
AA	(Very Strong)	CC	(Extremely Weak)
A	(Strong)	SD	(Selective Default)
BBB	(Good)	D	(Default)
BB	(Marginal)	R	(Regulatory Supervision)
B	(Weak)	NR	(Not Rated)

The ratings from 'AA' to 'CCC' may be modified by the addition of a plus (+) or minus (-) sign to show relative standing within the major rating categories. The rating scale above is in summary form. A full description of this rating scale can be obtained from www.standardandpoors.com.