PROPOSAL FORM – LONG

cyber event protection

emergence

Use this proposal form if any of the following apply:

- Your estimated revenue is >$25m, or
- You've requested a policy limit >$5m, or
- You've previously suffered a cyber loss, or
- You are in the IT, internet or telecommunications industry.

Completing this form requires technical knowledge of your IT. Consult with your IT manager or head of cyber security as necessary.

GENERAL

New Zealand Business Number (NZBN):

Name of policyholder:

Is the policyholder a subsidiary, franchisee or part of a larger group? ☐ Yes ☐ No

If Yes, please provide details:

Business activities:

Do you perform work for the defence industry or Government? ☐ Yes ☐ No

Policyholder's principal address:

Website(s) or domain(s):

List all domains for 'smarter cyber' monitoring or confirm: Don't know / don't have a website, domain or business email: ☐

Please provide the contact details of the person who is responsible for cyber security:

Note: This information will be used to provide critical security updates on a needs basis and will not be used for marketing purposes.

Name	Title
Email	Mobile

Total number of employees:

FINANCIALS

Estimated revenue for the coming 12 month period by territory:

		Are you located in the territory?
Australia/NZ	$	☐ Yes ☐ No
EU/UK	$	☐ Yes ☐ No
USA	$	☐ Yes ☐ No
Rest of world	$	☐ Yes ☐ No
Total	$ 0	

What percentage of total revenue is from online or e-commerce activities? %

DATA PROTECTION

1. Do you collect, process, hold or store data on behalf of any 3rd party? ☐ Yes ☐ No

2. Please state the total number of Personally Identifiable Information (PII) and other sensitive records you collect, process, hold or store in your business, including on behalf of others.
   Note: All categories of PII relating to the same individual (whether active or inactive) should only count as a single unique record.

   ☐ 0 - 25,000 ☐ 25,001 - 50,000 ☐ 50,001 - 75,000
   ☐ 75,001 - 100,000 ☐ 100,001 - 200,000 ☐ 200,001 - 300,000
   ☐ 300,001 - 400,000 ☐ 400,001 - 500,000 ☐ 500,001 - 750,000
   ☐ 750,001 - 1,000,000 ☐ 1,000,001 - 1,500,000 ☐ 1,500,001 - 2,000,000
   ☐ 2,000,001 - 2,500,000 ☐ 2,500,001 - 5,000,000 ☐ >5,000,000

   If >5,000,000 please provide the total number

3. Please select the type of records collected, processed, held or stored: (tick all that apply)

Customer information (e.g., name, address, email address, phone number etc)	☐ Yes ☐ No
Payment card information	☐ Yes ☐ No
Identity information (e.g., drivers licence, IRD number, passport number etc)	☐ Yes ☐ No
Banking or financial information	☐ Yes ☐ No
Medical or healthcare information	☐ Yes ☐ No
Biometric data	☐ Yes ☐ No
Trade secrets or intellectual property	☐ Yes ☐ No

4. Do you protect all personally identifiable information and other sensitive data through encryption while: (tick all that apply)

At rest	☐ Yes ☐ No
In transit	☐ Yes ☐ No
Backed up	☐ Yes ☐ No
Stored on portable devices	☐ Yes ☐ No
Stored with 3rd parties	☐ Yes ☐ No

5. Do you have the following policies in place? (tick all that apply)

   ☐ Privacy policy ☐ Cookies policy ☐ Data retention and data destruction policy
   ☐ Bring your own device policy that ensures data on portable devices is encrypted

GOVERNANCE

6. How frequently do you provide security awareness training to your employees?
   ☐ Annually ☐ Quarterly ☐ Monthly ☐ Not provided

7. How frequently do you test employees' security awareness through simulated phishing campaigns?
   ☐ Annually ☐ Quarterly ☐ Monthly ☐ Not provided

ASSET SECURITY

8. Do you maintain an inventory of all your hardware and software?

Hardware	☐ Yes ☐ No
Software	☐ Yes ☐ No

ASSET SECURITY (CONTINUED)

9. Have you implemented secure configurations to all hardware and software assets? ☐ Yes ☐ No

If Yes, please indicate which of the following have been implemented: (tick all that apply)

Changing and/or disabling default accounts and passwords	☐ Yes ☐ No
Disabling or removing unneeded services, components or features	☐ Yes ☐ No
Implementing vendor specific security recommendations	☐ Yes ☐ No
Enforcing encryption of local storage devices	☐ Yes ☐ No
Enable appropriate backups	☐ Yes ☐ No
Configure logging of system logons, activity, warnings and errors	☐ Yes ☐ No
Sending all logs to a centralised logging server	☐ Yes ☐ No
Assets are onboarded onto EDR and/or SIEM platforms	☐ Yes ☐ No

10. Have you deployed an Endpoint Detection and Response (EDR) tool that covers 100% of:

Servers?

☐ Yes, EDR covers 100%
☐ Yes, EDR covers 90% or more
☐ EDR covers less than 90%
☐ No, we have not deployed an EDR tool

Endpoints?

☐ Yes, EDR covers 100%
☐ Yes, EDR covers 90% or more
☐ EDR covers less than 90%
☐ No, we have not deployed an EDR tool

Indicate if AI/automated rules-based enforcement has been enabled: ☐ Yes ☐ No

If EDR has not been deployed or covers less than 90%, indicate what compensatory measures you've implemented: (tick all that apply)

Application whitelisting	☐ Yes ☐ No
Endpoint Protection Platform (EPP)	☐ Yes ☐ No
Next Generation Firewall (NGFW)	☐ Yes ☐ No
Intrusion Detection/Prevention System (IDS/IPS)	☐ Yes ☐ No
Content control software (web/URL filtering)	☐ Yes ☐ No
Other:	☐ Yes ☐ No

11. Have you implemented a critical security patch management process for your IT systems? ☐ Yes ☐ No

If Yes, how do you handle security patches?

☐ Manual updates, implemented within 30 days
☐ Manual updates, implemented within 90 days
☐ Manual updates, no time frame for implementation
☐ Devices are set to update software automatically (where available)

EMAIL SECURITY

12. Do you use an email filtration and scanning tool to authenticate emails and flag and quarantine suspicious content (e.g., executable files)? ☐ Yes ☐ No

IDENTITY AND ACCESS MANAGEMENT

13. Is Multi-Factor Authentication (MFA*) required for all users to access the following systems/platforms/services?

All remote access to the network?	☐ Yes ☐ No
Web-based email?	☐ Yes ☐ No
Admin/privilege service accounts?	☐ Yes ☐ No
Cloud resources, including back ups?	☐ Yes ☐ No

*Note: To qualify as multi-factor authentication, the authentication mechanism needs to be knowledge (something the user and only the user knows) and possession (something the user and only the user has). That way the compromise of any single device will only compromise a single authentication factor.

ASSESSMENTS

14. In the last 12 months have you had any of the following conducted on your business/systems? (tick all that apply)

Penetration test	☐ Yes ☐ No
Vulnerability scan	☐ Yes ☐ No
Payment Card Industry (PCI) assessment	☐ Yes ☐ No
External IT audit	☐ Yes ☐ No

END OF LIFE TECHNOLOGY

15. Do you rely on any operating system, software or hardware that is no longer supported or is considered end of life by the manufacturer? ☐ Yes ☐ No

If Yes, please answer the following questions:

Is any end of life technology internet facing?	☐ Yes ☐ No
Is it segregated from the rest of the network?	☐ Yes ☐ No
Has additional support been purchased where available?	☐ Yes ☐ No

Please outline any additional security measures that have been implemented to prevent exploitation of any vulnerabilities:

RESILIENCY AND RECOVERY

16. How frequently do you take regular backups of critical data and systems?
☐ Daily ☐ Weekly ☐ Monthly ☐ Greater than monthly

17. Do you keep a copy of critical backups offline, segregated from and inaccessible to your network? ☐ Yes ☐ No

18. Is your backup environment: (tick all that apply)

In the cloud	☐ Yes ☐ No
On premises	☐ Yes ☐ No
At a secondary, offsite data centre	☐ Yes ☐ No
Encrypted	☐ Yes ☐ No
MFA protected	☐ Yes ☐ No
Using immutable technology	☐ Yes ☐ No

19. How frequently do you test system restoration capabilities by performing a full restoration from a sample set of backup data? ☐ Annually ☐ Quarterly ☐ Monthly ☐ Not tested

20. Please confirm which of the following formal plans you have in place (which addresses cyber incidents) and whether tested at least annually:

	In place?	Tested annually?
Disaster Recovery Plan (DRP)	☐ Yes ☐ No	☐ Yes ☐ No
Business Continuity Plan (BCP)	☐ Yes ☐ No	☐ Yes ☐ No
Incident Response Plan (IRP)	☐ Yes ☐ No	☐ Yes ☐ No

Does your IRP specifically address ransomware scenarios? ☐ Yes ☐ No

PRIOR CLAIMS AND CIRCUMSTANCES

21. After enquiry, within the past 5 years, are you aware of any losses, claims, circumstances, cyber events, privacy breaches, regulatory investigations, crime or social engineering incidents which have impacted, or could adversely impact your business or give rise to a claim under a cyber policy? ☐ Yes ☐ No

1. Total impact, including all business interruption, remediation costs and other loss? $

Date of loss: / /

Please indicate the nature of the loss by ticking the appropriate box:

☐ Crime ☐ Data breach ☐ Denial of service
☐ Email compromise ☐ Hacking, malware ☐ Multimedia injury
☐ Ransomware ☐ Social engineering
☐ Other please describe:

What remediation steps and controls were implemented after the loss? (Attach report if available)

2. Total impact, including all business interruption, remediation costs and other loss? $

Date of loss: / /

Please indicate the nature of the loss by ticking the appropriate box:

☐ Crime ☐ Data breach ☐ Denial of service
☐ Email compromise ☐ Hacking, malware ☐ Multimedia injury
☐ Ransomware ☐ Social engineering
☐ Other please describe:

What remediation steps and controls were implemented after the loss? (Attach report if available)

22. Have you had any unforeseen down time to your website or IT network of more than 8 hours? ☐ Yes ☐ No

If Yes, provide details including duration, how resolved and any cost to you:

OPTIONAL COVER - NON-IT CONTINGENT BUSINESS INTERRUPTION AND SYSTEM FAILURE

23. Do you want Optional Cover for Non-IT Contingent Business Interruption and System Failure? ☐ Yes ☐ No

24. Tell us about your critical components, service providers and supplies.

☐ All critical components, services and supplies are readily available from multiple sources
☐ Substitutes can be available within 10 days
☐ Longer than 10 days for substitutes to be available
☐ Don't know
☐ Substituting components, services or supplies is not possible

OPTIONAL COVER - CRIMINAL FINANCIAL LOSS

25. Do you want Optional Cover for Criminal Financial Loss? ☐ Yes ☐ No

Includes cyber theft, telephone phreaking, identity-based theft, push payment theft and cryptojacking. Does not include socially engineered theft unless selected below.

26. Aggregate limit for Criminal Financial Loss

☐ $10,000 ☐ $25,000 ☐ $50,000 ☐ $75,000 ☐ $100,000 ☐ $150,000 ☐ $250,000 ☐ Other $

27. Excess applicable to Criminal Financial Loss only

☐ $0 ☐ $2,500 ☐ $5,000 ☐ $10,000 ☐ $15,000 ☐ $25,000 ☐ $50,000 ☐ $75,000 ☐ $100,000

☐ Other $

28. Do you want to include cover for socially engineered theft? ☐ Yes ☐ No

29. Sublimit for socially engineered theft

The sublimit for socially engineered theft is included within and cannot be greater than the aggregate limit for criminal financial loss. The excess for criminal financial loss applies to socially engineered theft as well.

☐ $5,000 ☐ $10,000 ☐ $15,000 ☐ $20,000 ☐ $30,000 ☐ $50,000

☐ $75,000 ☐ $100,000 ☐ $125,000 ☐ $150,000 ☐ $200,000 ☐ $250,000

30. Are all new payees, and changes to existing payees' banking details, double authenticated with the payee? ☐ Yes ☐ No

31. Do transfers > $10,000 require dual signature or supervisor / manager sign off? ☐ Yes ☐ No

32. After enquiry, have you within the past 5 years suffered a crime, fidelity or computer crime loss? ☐ Yes ☐ No

If Yes, please provide details:

OPTIONAL COVER - D&O LIABILITY

33. Do you want Optional Cover for Directors & Officers Liability? ☐ Yes ☐ No

D&O Liability is only available for unlisted companies.

34. Aggregate sublimit for D&O Liability ☐ $250,000 ☐ $500,000 ☐ $1,000,000

The sublimit for D&O Liability is included within and cannot be greater than the policy aggregate limit.

35. Are you listed on any stock exchange, or are you planning an initial public offering or any subsequent offering during the coming 12 months? ☐ Yes ☐ No

36. Have you within the past 5 years had D&O or Management Liability (ML) insurance declined or cancelled, or are you aware, after enquiry, of any D&O or ML loss, claim, or circumstance which has or could impact you or your business or give rise to a D&O or ML claim? ☐ Yes ☐ No

If Yes, please provide details:

OPTIONAL COVER - TANGIBLE PROPERTY

37. Do you want Optional Cover for Tangible Property? ☐ Yes ☐ No

The Tangible Property sublimit forms part of and is not in addition to the limit for Section C - Cyber Event Response Costs.

OPTIONAL COVER - JOINT VENTURE AND CONSORTIUM COVER

38. Do you want Optional Cover for your liability from joint ventures or consortia? ☐ Yes ☐ No

If Yes, provide the name(s) of the joint venture or consortium:

Note: You must also include your share of revenue from the JV or consortium for the coming 12 months in your estimated total revenue.

TRADING NAMES, SUBSIDIARIES AND AFFILIATES

39. If you wish to list trading names, please list them individually in the boxes provided below.

40. If you wish to list subsidiaries, please list them individually in the boxes provided below.

Note: Subsidiaries of the policyholder are automatically covered and do not require scheduling. Listing an entity here does not extend cover or affect cover in any way. This list is for your convenience only.

41. Do you require cover for affiliated companies? ☐ Yes ☐ No

If Yes, please list the affiliates and revenue below and tell us how you are affiliated and about the IT.

Note: Listing an entity here means you are submitting it to Emergence for consideration. Cover will only apply to those entities accepted by Emergence and scheduled on the policy. You must provide revenue estimates for each entity and include revenue from all affiliates for the coming 12 months in your total estimated revenue.

Affiliate 1: Revenue $

Nature of affiliation: ☐ Authorised rep ☐ Family business ☐ Franchisee ☐ Shared directorships ☐ Other:

Is this affiliate's IT fully separate and independent? ☐ Yes ☐ No

If not, please describe any shared IT:

Affiliate 2: Revenue $

Nature of affiliation: ☐ Authorised rep ☐ Family business ☐ Franchisee ☐ Shared directorships ☐ Other:

Is this affiliate's IT fully separate and independent? ☐ Yes ☐ No

If not, please describe any shared IT:

You can include here other information or facts you would like to bring to the underwriter's attention:

PLEASE SPECIFY YOUR PREFERRED EXCESS, INDEMNITY PERIOD AND AGGREGATE LIMIT

Excess

☐ $0 ☐ $2,500 ☐ $5,000 ☐ $10,000 ☐ $15,000 ☐ $25,000 ☐ $50,000 ☐ Other $

Section A indemnity period

☐ 30 days ☐ 60 days ☐ 90 days ☐ 180 days ☐ 365 days

Policy aggregate limit

☐ $250,000 ☐ $500,000 ☐ $1,000,000 ☐ $2,000,000 ☐ $3,000,000 ☐ $4,000,000

☐ $5,000,000 ☐ $10,000,000 ☐ Other $

DECLARATION

I/we acknowledge that:

1. I/we have read and understood the important information provided on the last page of this document in the important information section.
2. I/we are authorised by all those seeking insurance to make this proposal, and declare all information on this proposal and any attachment is true and correct.
3. I/we authorise the underwriter to give to, or obtain from, other insurers or any credit reference service, any information relating to insurance held by me/us or any claim in relation thereto.
4. I/we acknowledge that, where answers are provided in the proposal are not in my/our handwriting, I/we have checked and certify that the answers are true and correct.

Policyholder's signature: Date: / /

GLOSSARY

Admin/privilege service accounts

Admin/privileged accounts refer to user accounts that have elevated privileges.

Admin accounts can manage and maintain a system or network.

Privileged accounts are used for automated processes or by applications that require elevated privileges to perform a task.

AI/automated rules-based enforcement

AI/automated rules-based enforcement is a mechanism designed to enforce predefined rules within security systems. An automated rules-based system is actively monitoring and enforcing certain rules or conditions to respond to a security threat.

Application whitelisting

Application whitelisting allows only authorised and approved applications to run on a system or network.

Content control software

Content-control software, commonly referred to as an Internet filter, is software that restricts or controls the content a user is able to access and/or download via the Internet.

Domain

A domain name (often called a domain) is an easy-to-remember name that's associated with a physical IP address on the Internet. It's the unique name that appears after the @ symbol in email addresses, and after www. in web addresses. Examples of domain names include google.com and wikipedia.org.

E-commerce activities

E-commerce involves the sale of goods and services over the internet. For example, online retail stores, digital products (e-books, music) and online marketplaces (eBay, Amazon etc).

Encryption

Encryption is the process of converting information or data into code to prevent unauthorised use.

Encryption at rest refers to encrypting data when it is stored on a device or storage system.

Encryption in transit refers to encrypting data as it travels across a network or between systems.

End of Life technology (EOL)

EOL refers to a stage in the life cycle of a technology product where it is no longer developed, maintained or supported by the manufacturer.

Endpoint Detection and Response (EDR)

EDR technology focuses on the detection, investigation, and mitigation of suspicious activities on endpoints including computers, servers and other devices within a network. EDR can identify anomalies and identify potential security threats.

Endpoint Protection Platform (EPP)

EPP is designed to defend endpoints such as laptops, servers and other devices connected to a network from various forms of malicious activities including malware, ransomware, and other cyber threats.

Intrusion Detection Systems (IDS) and Intrusion Prevention System (IPS)

IDS and IPS are technologies designed to detect and respond to malicious activities or security incidents within a computer network. IDS is used to monitor a network or system and identify patterns or behaviours that may indicate unauthorised access. IPS goes a step further than IDS by automatically blocking detected threats.

Immutable technology

Immutable technology is a type of technology or system where data or code cannot be altered or modified once it is created or deployed.

Multi-Factor Authentication (MFA)

MFA is a mechanism that requires individuals to provide more than one form of identification to access an account or system. The additional forms of identification can include one-time codes or biometrics.

Next Generation Firewall (NGFW)

NGFW combines traditional firewall capabilities with advanced functionalities such as application awareness, intrusion prevention, user identity awareness and advanced threat detection.

Payment Card Industry (PCI) assessment

PCI assessment is a process designed to evaluate a companies handling of credit card transactions to ensure a company complies with the PCI security standards.

Security Information and Event Management (SIEM)

A SIEM system provides real time analysis of logs that are gathered from various sources such as servers and security applications. A SIEM system will analyse the logs and identify potential security incidents.

Security patch management process

A security patch management process involves applying patches or updates to software and systems at regular intervals to address vulnerabilities and protect against security threats.

emergence

It is important that you read and understand the following.

Claims made notice

Section B – Loss to Others of this policy is issued on a 'claims made and notified' basis. This means that Section B – loss to others responds to:

a. claims first made against you during the policy period and notified to us during the policy period, provided that you were not aware at any time prior to the commencement of the policy of circumstances which would have put a reasonable person in your position on notice that a claim may be made against him/her; and:

b. facts that you may decide to notify are those which might give rise to a claim against you even if a claim has not yet been made against you. Such notification must be given as soon as reasonably practicable after you become aware of the facts and prior to the expiry of the policy period. If you give written notification of facts the policy will respond even though a claim arising from those facts is not made against you until after the policy has expired. When the policy period expires, no new notification of facts can be made to us on the expired policy for a cyber event first discovered or identified by you during the policy period.

Your duty of disclosure

When you apply for insurance you have a legal duty of disclosure. This means you or anyone applying on your behalf must tell us everything you know (or could be reasonably expected to know) that might affect our decision when deciding:

a. to accept your insurance, and/or

b. the cost or terms of the insurance, including the excess.

c. In particular, you should tell us anything which may increase the chance of a claim under this policy, or the amount of a claim under this policy.

You also have this duty every time your insurance renews and when you make any changes to it. If you or anyone on your behalf breaches this duty of disclosure, we may treat this policy as being of no effect and to have never existed.

Please ask us if you are not sure whether you need to tell us about something.

About Emergence NZ Limited

Emergence NZ Limited (NZBN: 9429051153861, FSP: 1005174) ('Emergence') acts under a binding authority given to it by the insurer to administer and issue policies, alterations and renewals. In all aspects of arranging this policy, Emergence acts as an agent for the insurer and not for you.

Contact details are:

Email: info@emergenceins.co.nz

Telephone: 0800 129 237 (0800 1 CYBER)

Postal address: Level 11, Shortland Centre, 55 Shortland Street, Auckland 1010