# Cyber Event Protection Proposal Form

emergence

Policyholder / Business Name

Business Activity, Industry or Profession

New Zealand Business Number (NZBN)

Policyholder's Principal Address (Suburb, Postcode)

Trading Names

Affiliates

Websites

Please provide your estimated Revenue for the coming 12 month period by region, and indicate in which territories you are located.

| Region | Revenue | In which territories are you located? | | |
|---|---|---|---|---|
| NZ/Aus | $ | NZ/Aus | Yes | No |
| EU/UK | $ | EU/UK | Yes | No |
| USA | $ | USA | Yes | No |
| Rest of World | $ | Rest of World | Yes | No |
| **Total Revenue** | $ | | | |

1. Estimated annual total number of transactions and records

   Combined number of client/ customer records and total number of credit card transactions.

- ☐ 0 - 10,000
- ☐ 10,001 - 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:

2. Do you comply with your relevant PCI DSS obligations?

- ☐ Yes
- ☐ No
- ☐ Don't Know
- ☐ N/A - We are not subject to PCI DSS.

3. What percentage of your Total Revenue is from online or e-commerce activities? %

# Cyber Event Protection Proposal Form

emergence

| | | | |
|---|---|---|---|
| 4. Number of full time employees | ☐ 1 - 10<br>☐ 31 - 50<br>☐ > 200 | ☐ 11 - 20<br>☐ 51 - 100<br>If >200, please provide the number: | ☐ 21 - 30<br>☐ 101 - 200 |
| 5. Do you have a Notifiable Data Breach plan in place and otherwise comply with *The Privacy Act*? | ☐ Yes<br>☐ Don't Know | ☐ No<br>☐ N/A - We are not subject to the Privacy Act. | |
| 6. Do you have a Data Protection/Privacy policy? | ☐ Yes | ☐ No | ☐ Don't Know |
| 7. Do you have firewalls protecting your own and customer/client data? | ☐ Yes | ☐ No | ☐ Don't Know |
| 8. Do you protect all Personally Identifiable Information and other sensitive data through Encryption? | ☐ Yes, info encrypted at rest on our network, in transit and when backed-up<br>☐ Yes, info encrypted in transit and when backed up but not when at rest on our network<br>☐ Yes, info encrypted but ONLY in specific limited scenarios<br>☐ No, info not encrypted whatsoever | | |
| 9. Do you outsource the handling of any Personally Indentifiable Information? | ☐ Yes | ☐ No | ☐ Don't Know |
| 10. Do you use up-to date antivirus/spyware and malware software? | ☐ Yes, updated daily or automatically upon release<br>☐ Yes, updated on a weekly to monthly basis | | ☐ No<br>☐ Don't Know |
| 11. Are all mission/business critical systems and data information assets backed up and stored at another location? | ☐ Yes, backed up daily<br>☐ Yes, backed up weekly or less frequently | | ☐ No<br>☐ Don't Know |
| 12. Has an independent party completed an audit of your system/data security? | ☐ Yes | ☐ No | ☐ Don't Know |
| 13. If your IT network failed, which of the following would best describe the impact to your operations and revenues? | ☐ Inconvenience, very minimal revenue impact and operations could continue temporarily<br>☐ Revenues would NOT be impacted immediately, and only slightly when impacted<br>☐ Revenues would NOT be impacted immediately, but significantly when impacted<br>☐ Revenues would be impacted immediately but only slightly<br>☐ Revenues would be impacted immediately and significantly<br>☐ Operations and revenues would be entirely interrupted | | |
| 14. Do you have written data security policies and procedures communicated to all employees, and do employees receive annual security awareness training? | ☐ Yes, both written policies plus annual security awareness training<br>☐ Written policies but no employee security awareness training<br>☐ Employee security awareness training but no written security policies<br>☐ No<br>☐ Don't Know | | |
| 15. Are you aware of any claims, circumstances, privacy breaches, viruses, DoS / DDoS, or hacking incidents which have impacted, or could adversely impact your business? | ☐ Yes<br>If yes, please provide details including costs incurred and any remedial action taken | | ☐ No |

Answer questions on this page if:
- Your Estimated Revenue is >$25m,
- You've requested a Policy Limit >$5m, **or**
- You have suffered a previous cyber loss

emergence

1. Describe the type of information in records held by you:
   Tick all that apply
   - ☐ Customer info (e.g., Name, Address, E-Mail Address, Phone, etc.)
   - ☐ Credit card details
   - ☐ Personal Identity info (e.g., Drivers License, TFN, IDR Passport #, Gov't ID)
   - ☐ Confidential 3rd party trade secrets or IP (Intellectual Property)
   - ☐ Banking or Financial details
   - ☐ Medical or Healthcare data

2. Do you have a dedicated person responsible for your IT infrastructure, data security and privacy?
   - ☐ Yes, full time IT Manager, Chief Information Security Officer (CISO) or similar
   - ☐ Outsourced - IT contractor provides a full time dedicated person
   - ☐ No, responsibility is shared amongst Legal, HR and other departments
   - ☐ No
   - ☐ Don't know

3. Do you have a Disaster Recovery Plan (DRP) and/or Business Continuity Plan (BCP) in place and has this been tested in the last 18 months?
   - ☐ Yes, current and tested
   - ☐ Yes, but not ever tested
   - ☐ Yes, but not tested in the past 18 months
   - ☐ No

4. Does your network include contingency / redundancy / resilience of any description, to mitigate system interruptions or failures (such as mirrored infrastructure, failover mechanisms, warm or hot replicated sites or similar)?
   - ☐ Yes, multiple aspects
   - ☐ Yes, but just one aspect
   - ☐ No

5. Do you control / limit / monitor your employees' ability to remove data or information from your network / office (examples include USB drive security)?
   - ☐ Yes, for data and physical information
   - ☐ Yes, for physical information only
   - ☐ Yes, for data only
   - ☐ No

6. Does your website use Web Apps?
   - ☐ Yes
   - ☐ Don't Know
   - ☐ No
   - ☐ N/A - we do not have a website

7. Do you use monitored Intrusion Detection or Intrusion Prevention Systems (IDS/IPS)?
   - ☐ Yes
   - ☐ No
   - ☐ Don't Know

8. Are you aware of any evidence of network intrusion or vulnerabilities highlighted in an IT Security audit or Penetration test which have not yet been resolved?
   - ☐ Yes
   - ☐ No

   If yes, please provide details

9. Have you had any unforeseen down time to your website or IT network of more than 12 hours?
   - ☐ Yes
   - ☐ No

   If yes, please provide details

Answer questions on this page if:
- Your Estimated Revenue is >$75m,
- You've requested a Policy Limit >$5m, **or**
- You have suffered a previous cyber loss

emergence

| E-MAIL, RDP, O365 | | |
|---|---|---|
| 1. Do you authenticate outbound email?<br>If Yes, indicate how. If no, tick No. | ☐ DMARC<br>☐ DKIM<br>☐ SPF | ☐ No<br>☐ Don't Know |
| 2. Do you scan and filter inbound emails for malicious content (e.g., executable files)? | ☐ Yes | ☐ No<br>☐ Don't Know |
| 3. Does all remote access to your network and corporate email require multifactor authentication (MFA)? | ☐ Yes | ☐ No<br>☐ Don't know |
| 4. Have you disabled remote desktop protocol (RDP)? | ☐ Yes | ○ No<br>○ Don't know |
| If No, have you implemented any of the following: | ☐ VPN<br>☐ MFA | ☐ RDP Honeypots<br>☐ None of these |
| 5. Do you use O365 or Microsoft 365 in your organisation? | ☐ Yes | ☐ No<br>☐ Don't know |
| If Yes, indicate if any of the following have been implemented: | ☐ MFA<br>☐ ATP | ☐ Macros disabled by default |
| If No, which product do you use for email monitoring (e.g. Proofpoint): | | |
| 6. Do you train end users against phishing and social engineering threats via ongoing campaigns and assessments? | ☐ Yes, Annually<br>☐ Yes, Quarterly<br>☐ Yes, Monthly | ☐ No<br>☐ Don't Know |

| Backups | | |
|---|---|---|
| 7. Do you take regular backups of critical data? | ☐ Yes | ☐ No<br>☐ Don't Know |
| If Yes, how frequently? | ☐ Daily<br>☐ Monthly | ☐ Weekly<br>☐ Other |
| 8. Do you keep a copy of critical backups offline, segregated from and inaccessible to your network? | ☐ Yes | ☐ No<br>☐ Don't Know |
| 9. Where do you store backups? | ☐ Cloud<br>☐ Offline | ☐ At a Secondary Data Centre<br>☐ In a separate network segment |
| 10. Which of the following have been implemented to secure the backup environment? | ☐ Encryption<br>☐ Vaulted Credentials | ☐ Segmentation<br>☐ MFA<br>☐ None of these |
| 11. Do you use any commercial backup solutions (e.g. Commvault)? | ☐ Yes | ☐ No<br>☐ Don't Know |
| If Yes, Which product(s) do you use: | | ☐ Don't Know |

Answer questions on this page if:
- Your Estimated Revenue is >$75m,
- You've requested a Policy Limit >$5m, **or**
- You have suffered a previous cyber loss

emergence

## Backups continued

| | | | |
|---|---|---|---|
| 12. Does your backup strategy include the use of immutable technologies? | ☐ Yes | ☐ No | ☐ Don't Know |
| 13. Is the integrity of these backups and your recovery plans regularly tested? | ☐ Yes | ☐ No | ☐ Don't Know |

## Perimeter defence & privileges

| | | |
|---|---|---|
| 14. Do you use an endpoint protection product (EPP)? | ☐ Yes | ☐ No<br>☐ Don't Know |
| If Yes, which product(s): | | ☐ Don't Know |
| 15. Have you deployed an endpoint detection and response (EDR) tool that covers 100% of Servers and Endpoints? | ☐ Yes - Servers<br>☐ Yes - Endpoints | ☐ No<br>☐ Don't Know |
| If so, which product(s) do you use? | | ☐ Don't Know |
| If the EDR tool offers AI/automated rules-based enforcement, has this been enabled? | ☐ Yes<br>☐ N/A | ☐ No<br>☐ Don't Know |
| 16. Do you operate a SIEM monitored 24/7/365 by an internal SOC or MSSP? | ☐ Yes | ☐ No ☐ Don't Know |
| 17. Do you enforce a BYOD (Bring Your Own Device) policy that ensures critical data is encrypted when transferred to portable media devices (USBs, Laptops etc)? | ☐ Yes | ☐ No ☐ Don't Know |
| 18. Do you allow local administrator rights on workstations? | ☐ Yes | ☐ No ☐ Don't Know |
| 19. Do administrative/privileged accounts utilise a privilege access management (PAM) tool (e.g. CyberArk)? | ☐ Yes | ☐ No ☐ Don't Know |
| If Yes, which product do you use? | | ☐ Don't Know |

## Incident response plan

| | | |
|---|---|---|
| 20. Does your incident response plan (IRP) specifically address ransomware scenarios? | ☐ Yes<br>☐ No | ☐ Don't Know<br>☐ We don't have an IRP |

If NO to any of the above, please detail below along with mitigating comments:

Please outline any additional controls your organisation has in place to mitigate the threat of ransomware attacks (e.g. tagging of external emails, use of unique credentials, vulnerability scanning, etc.):

# Cyber Event Protection
# Optional Covers

emergence

## OPTIONAL COVER - Contingent Business Interruption

1. Do you want Optional Cover for Contingent Business Interruption?
   - ☐ Yes
   - ☐ No

2. 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

1. Do you want Optional Cover for Criminal Financial Loss?

   Includes Cyber Theft, Telephone Phreaking, Identity-based Theft, Push Payment Theft and Cryptojacking. Does not include Socially Engineered Theft unless selected below.
   - ☐ Yes
   - ☐ No

2. Aggregate Limit for Criminal Financial Loss
   - ☐ $10,000
   - ☐ $25,000
   - ☐ $50,000
   - ☐ $75,000
   - ☐ $100,000
   - ☐ $150,000
   - ☐ $250,000
   - ☐ Other $

3. Do you want to include cover for Socially Engineered Theft?
   - ☐ Yes
   - ☐ No

4. Sublimit for Socially Engineered Theft
   The sublimit for Socially Engineered Theft cannot be greater than the aggregate limit for Criminal Financial Loss.
   - ☐ $5,000
   - ☐ $10,000
   - ☐ $15,000
   - ☐ $20,000
   - ☐ $30,000
   - ☐ $50,000
   - ☐ $75,000
   - ☐ $100,000
   - ☐ $125,000
   - ☐ $150,000
   - ☐ $200,000
   - ☐ $250,000

5. Do you require passwords to be changed regularly (at least quarterly)?
   - ☐ Yes
   - ☐ No
   - ☐ Don't Know

6. Do you allow remote access to your internal network?
   - ☐ Yes
   - ☐ Yes, with dual authentication
   - ☐ No
   - ☐ Don't know

7. Are all new payees, and changes to existing payees' banking details, double authenticated with the payee?
   - ☐ Yes
   - ☐ No
   - ☐ Don't Know

8. Do transfers > $10,000 require dual signature or supervisor / manager sign off?
   - ☐ Yes
   - ☐ No
   - ☐ Don't Know

9. Are you entrusted with or in control of funds from a 3rd party, or do you provide any of the following services for others?

   Tick all that apply
   - ☐ Collection or payment processing?
   - ☐ Asset, investment or trust management services?
   - ☐ Cash management or other treasury functions?
   - ☐ Other office functions?

   If 'Other', please provide details

# Cyber Event Protection
# Optional Covers

emergence

10. Have you ever been declined for Crime, Fidelity or Computer Crime insurance, or had such insurance cancelled?

☐ Yes ☐ No ☐ N/A - have never had such insurance

If yes, please provide details

11. Have you ever suffered a Crime, Fidelity or Computer Crime loss?

☐ Yes ☐ No

If yes, please provide details

## OPTIONAL COVER - Tangible Property

1. Do you want Optional Cover for Tangible Property?

☐ Yes ☐ No

2. Aggregate Limit for Tangible Property

☐ $5,000 ☐ $10,000 ☐ $15,000
☐ $25,000 ☐ $50,000 ☐ Other $

## OPTIONAL COVER - Joint Venture and Consortium Cover

1. Do you want Optional Cover for your liability from Joint Ventures or Consortia? 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.

☐ Yes ☐ No

## Please specify your preferred excess, indemnity period and aggregate limit

Excess

☐ $250 ☐ $1,000 ☐ $2,500
☐ $5,000 ☐ $10,000 ☐ $15,000
☐ $25,000 ☐ 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 $

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 |
|---|---|

# Important Information

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