

Cyber Event Protection Proposal Form

emergence

Policyholder / Business Name

Business Activity, Industry or Profession

Australian Business No. (ABN)

Policyholder's Principal Address (Suburb, State, Postcode)

Trading Names/
Affiliates

Websites

Are you exempt from Stamp Duty? Yes No

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?		
Australia/NZ	\$	Australia/NZ	<input type="checkbox"/> Yes	<input type="checkbox"/> No
EU/UK	\$	EU/UK	<input type="checkbox"/> Yes	<input type="checkbox"/> No
USA	\$	USA	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Rest of World	\$	Rest of World	<input type="checkbox"/> Yes	<input type="checkbox"/> 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.	<input type="checkbox"/> 0 - 10,000	<input type="checkbox"/> 10,001 - 25,000	<input type="checkbox"/> 25,001 - 50,000
	<input type="checkbox"/> 50,001 - 75,000	<input type="checkbox"/> 75,001 - 100,000	<input type="checkbox"/> 100,001 - 200,000
	<input type="checkbox"/> 200,001 - 300,000	<input type="checkbox"/> 300,001 - 400,000	<input type="checkbox"/> 400,001 - 500,000
	<input type="checkbox"/> 500,001 - 750,000	<input type="checkbox"/> 750,001 - 1,000,000	<input type="checkbox"/> 1,000,001 - 1,500,000
	<input type="checkbox"/> 1,500,001 - 2,000,000	<input type="checkbox"/> 2,000,001 - 2,500,000	<input type="checkbox"/> 2,500,001 - 5,000,000
	<input type="checkbox"/> >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

4. Number of full time employees	<input type="checkbox"/> 1 - 10 <input type="checkbox"/> 31 - 50 <input type="checkbox"/> > 200	<input type="checkbox"/> 11 - 20 <input type="checkbox"/> 51 - 100 If >200, please provide the number:	<input type="checkbox"/> 21 - 30 <input type="checkbox"/> 101 - 200 <input type="text"/>
5. Do you have a Notifiable Data Breach plan in place and otherwise comply with <i>The Privacy Act 1988</i> ?	<input type="checkbox"/> Yes <input type="checkbox"/> Don't Know	<input type="checkbox"/> No <input type="checkbox"/> N/A - We are not subject to the Privacy Act.	
6. Do you have a Data Protection/Privacy policy?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Don't Know
7. Do you have firewalls protecting your own and customer/client data?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Don't Know
8. Do you protect all Personally Identifiable Information and other sensitive data through Encryption?	<input type="checkbox"/> Yes, info encrypted at rest on our network, in transit and when backed-up <input type="checkbox"/> Yes, info encrypted in transit and when backed up but not when at rest on our network <input type="checkbox"/> Yes, info encrypted but ONLY in specific limited scenarios <input type="checkbox"/> No, info not encrypted whatsoever		
9. Do you outsource the handling of any Personally Identifiable Information?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Don't Know
10. Do you use up-to date antivirus/spyware and malware software?	<input type="checkbox"/> Yes, updated daily or automatically upon release <input type="checkbox"/> Yes, updated on a weekly to monthly basis	<input type="checkbox"/> No <input type="checkbox"/> Don't Know	
11. Are all mission/business critical systems and data information assets backed up and stored at another location?	<input type="checkbox"/> Yes, backed up daily <input type="checkbox"/> Yes, backed up weekly or less frequently	<input type="checkbox"/> No <input type="checkbox"/> Don't Know	
12. Has an independent party completed an audit of your system/data security?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Don't Know
13. If your IT network failed, which of the following would best describe the impact to your operations and revenues?	<input type="checkbox"/> Inconvenience, very minimal revenue impact and operations could continue temporarily <input type="checkbox"/> Revenues would NOT be impacted immediately, and only slightly when impacted <input type="checkbox"/> Revenues would NOT be impacted immediately, but significantly when impacted <input type="checkbox"/> Revenues would be impacted immediately but only slightly <input type="checkbox"/> Revenues would be impacted immediately and significantly <input type="checkbox"/> 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?	<input type="checkbox"/> Yes, both written policies plus annual security awareness training <input type="checkbox"/> Written policies but no employee security awareness training <input type="checkbox"/> Employee security awareness training but no written security policies <input type="checkbox"/> No <input type="checkbox"/> 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?	<input type="checkbox"/> Yes	<input type="checkbox"/> No If yes, please provide details including costs incurred and any remedial action taken	<input type="text"/>

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

1. Describe the type of information in records held by you: Tick all that apply	<input type="checkbox"/> Customer info [e.g., Name, Address, E-Mail Address, Phone, etc.]
	<input type="checkbox"/> Credit card details
	<input type="checkbox"/> Personal Identity info [e.g., Drivers License, TFN, Passport #, Gov't ID]
	<input type="checkbox"/> Confidential 3rd party trade secrets or IP [Intellectual Property]
	<input type="checkbox"/> Banking or Financial details
	<input type="checkbox"/> Medical or Healthcare data
2. Do you have a dedicated person responsible for your IT infrastructure, data security and privacy?	<input type="checkbox"/> Yes, full time IT Manager, Chief Information Security Officer (CISO) or similar
	<input type="checkbox"/> Outsourced - IT contractor provides a full time dedicated person
	<input type="checkbox"/> No, responsibility is shared amongst Legal, HR and other departments
	<input type="checkbox"/> No
	<input type="checkbox"/> 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?	<input type="checkbox"/> Yes, current and tested
	<input type="checkbox"/> Yes, but not ever tested
	<input type="checkbox"/> Yes, but not tested in the past 18 months
	<input type="checkbox"/> 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]?	<input type="checkbox"/> Yes, multiple aspects
	<input type="checkbox"/> Yes, but just one aspect
	<input type="checkbox"/> No
5. Do you control / limit / monitor your employees' ability to remove data or information from your network / office [examples include USB drive security]?	<input type="checkbox"/> Yes, for data and physical information
	<input type="checkbox"/> Yes, for physical information only
	<input type="checkbox"/> Yes, for data only
	<input type="checkbox"/> No
6. Does your website use Web Apps?	<input type="checkbox"/> Yes
	<input type="checkbox"/> No
	<input type="checkbox"/> Don't Know
	<input type="checkbox"/> N/A - we do not have a website
7. Do you use monitored Intrusion Detection or Intrusion Prevention Systems [IDS/IPS]?	<input type="checkbox"/> Yes
	<input type="checkbox"/> No
	<input type="checkbox"/> 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?	<input type="checkbox"/> Yes
	<input type="checkbox"/> No
	If yes, please provide details
	<div style="border: 1px solid #ccc; height: 100px;"></div>
9. Have you had any unforeseen down time to your website or IT network of more than 12 hours?	<input type="checkbox"/> Yes
	<input type="checkbox"/> No
	If yes, please provide details
	<div style="border: 1px solid #ccc; height: 100px;"></div>

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

E-MAIL, RDP, O365

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

Backups

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

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	Don't Know
If Yes, which product(s):	<input type="text"/>		Don't Know
15. Have you deployed an endpoint detection and response [EDR] tool that covers 100% of Servers and Endpoints?	Yes - Servers Yes - Endpoints	No	Don't Know
If so, which product(s) do you use?	<input type="text"/>		Don't Know
If the EDR tool offers AI/automated rules-based enforcement, has this been enabled?	Yes N/A	No	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?	<input type="text"/>		Don't Know

Incident response plan

20. Does your incident response plan [IRP] specifically address ransomware scenarios?	Yes	Don't Know
	No	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.]:

OPTIONAL COVER - Contingent Business Interruption

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

- 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

- Do you want Optional Cover for Criminal Financial Loss? Yes No
 Includes Cyber Theft, Telephone Phreaking, Identity-based Theft and Cryptojacking. Does not include Socially Engineered Theft unless selected below.

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

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

- 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

- Do you require passwords to be changed regularly [at least quarterly]? Yes No Don't Know

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

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

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

- 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

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. Yes No

NOTE: You must also include your share of revenue from the JV or consortium for the coming 12 months in your Estimated Total Revenue.

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

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:

- 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
- written notification of facts pursuant to Section 40(3) of the *Insurance Contracts Act 1984 (Cth)*. Effectively, the 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

Before you enter into an insurance contract, you have a duty to tell us anything that you know, or could reasonably be expected to know, may affect our decision to insure you and on what terms. You have this duty until we agree to insure you.

You have the same duty before you renew, extend, vary, continue under similar insurance or reinstate an insurance policy.

You do not need to tell us anything that:

- reduces the risk we insure you for; or

- is common knowledge; or
- we know or should know as an insurer; or
- we waive your duty to tell us about.

If you do not tell us anything you are required to, we may cancel your policy or reduce the amount we will pay you if you make a claim, or both

If your failure to tell us is fraudulent, we may refuse to pay a claim and treat the policy as if it never existed.

About Emergence Insurance Pty Ltd

Emergence Insurance Pty Ltd (ABN 46 133 037 153, AFSL 329634) ('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@emergenceinsurance.com.au

Telephone: +61 2 8280 3000

Postal address: PO Box A2016 Sydney South NSW 1235

Privacy

In this Privacy Notice the use of "we", "our" or "us" means the insurer and Emergence, unless specified otherwise.

We are committed to protecting your privacy.

We need to collect, use and disclose your personal information [which may include sensitive information] in order to consider your application for insurance and to provide the cover you have chosen, administer the insurance and assess any claim. You can choose not to provide us with some of the details or all of your personal information, but this may affect our ability to provide the cover, administer the insurance or assess a claim.

The primary purpose for our collection and use of your personal information is to enable us to provide insurance services to you.

Personal information will be obtained from individuals directly where possible and practicable to do so. Sometimes it may be collected indirectly (e.g. from your insurance intermediary or co-insureds). If you provide personal information for another person you represent to us that:

- you have the authority from them to do so and it is as if they provided it to us;
- you have made them aware that you will or may provide their personal information to us, the types of third parties we may provide it to, the relevant purposes we and the third parties we disclose it to will use it for, and how they can access it. If it is sensitive information we rely on you to have obtained their consent on these matters. If you have not done or will not do either of these things, you must tell us before you provide the relevant information.

We may disclose the personal information we collect to third parties who assist us in providing the above services, such as related entities, distributors, agents, insurers, reinsurers and service providers. Some of these third parties may be located

outside of Australia. In all instances where personal information may be disclosed to third parties who may be located overseas, we will take reasonable measures to ensure that the overseas recipient holds and uses your personal information in accordance with the consent provided by you and in accordance with our obligations under *The Privacy Act 1988 (Cth)*.

In dealing with us, you consent to us using and disclosing your personal information as set out in this statement. This consent remains valid unless you alter or revoke it by giving written notice to Emergence's Privacy Officer. However, should you choose to withdraw your consent, we may not be able to provide insurance services to you.

The Emergence Privacy Policy available at www.emergenceinsurance.com.au or by calling Emergence, sets out how:

- Emergence protects your personal information;
- you may access your personal information;
- you may correct your personal information held by us;
- you may complain about a breach of *The Privacy Act 1988 (Cth)* or Australian Privacy Principles and how Emergence will deal with such a complaint.

If you would like additional information about privacy or would like to obtain a copy of the Privacy Policy, please contact the Emergence Privacy Officer by:

Postal Address: PO Box A2016, Sydney South NSW 1235

Phone: +61 2 9307 6656

Fax: +61 2 9307 6699

Email: privacyofficer@steadfastagencies.com.au

You can download a copy of the Emergence Privacy Policy by visiting www.emergenceinsurance.com.au.