

Cyber Event Protection Proposal Form

EMERGENCY

If turnover is less than \$25m, please answer the first 2 pages.
Optional Coverages are on page 3.
If turnover is greater than \$25m, please complete page 4 as well.

Insured Entity	
Business / Trading Name	
Business Description, Industry or Profession	
Website address	
Business Address (Suburb, State, Postcode)	

Estimated Total Sales for the coming 12 month period

\$

What percentage of your Total Sales is from online or e-commerce activities?

%

Annual Aggregate Policy Limit

Number of full time employees

1- 10

11 -20

21-30

31-50

> 50

Please provide the number:

Section A Indemnity Period

30 days

60 days

90 days

180 days

365 days

Excess

\$250

\$1,000

Other

\$2,500

\$5,000

\$

Cyber Event Protection Proposal Form

EMERGENCE

1. Estimated annual total number of transactions and records <i>Combined number of clients/customer records and total number of credit card transactions.</i>	<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 - 250,000
	<input type="checkbox"/> 250,001 - 500,000	<input type="checkbox"/> 500,001 - 999,999	<input type="checkbox"/> 1,000,000+
2. Do you comply with your relevant PCI DSS obligations?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Don't Know
	<input type="checkbox"/> Don't Know	<input type="checkbox"/> N/A - We are not subject to PCI DSS.	
3. Do you comply with The Privacy Act 1988 (Privacy Act)?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Don't Know
	<input type="checkbox"/> Don't Know	<input type="checkbox"/> N/A - We are not subject to the Privacy Act.	
4. Do you have a Data Protection/Privacy policy?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Don't Know
5. 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
6. 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		
7. Do you outsource the handling of any Personally Identifiable Information?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> Don't Know
8. 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		
9. 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		
10. 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
11. Do you have written data safety policies and procedures and do employees receive annual security awareness training?	<input type="checkbox"/> Yes, both written policies plus annual security awareness training <input type="checkbox"/> Employee security awareness training but no written security policies <input type="checkbox"/> Written policies but no employee security awareness training <input type="checkbox"/> No <input type="checkbox"/> Don't Know		
12. If your IT network failed, which of the following would best describe the impact to your business?	<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		
13. Are you aware of any claims, circumstances, privacy breaches, viruses, 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 <div style="border: 1px solid black; height: 20px; width: 100%;"></div>		

OPTIONAL COVER - Contingent Business Interruption

- | | | |
|--|--|-----------------------------|
| 1. Do you want Optional Cover for Contingent Business Interruption? | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
| 2. Tell us about your critical components, service providers and supplies. | <input type="checkbox"/> All critical components, services and supplies are readily available from multiple sources
<input type="checkbox"/> Substitutes can be available within 10 days
<input type="checkbox"/> Longer than 10 days for substitutes to be available
<input type="checkbox"/> Don't know
<input type="checkbox"/> Substituting components, services or supplies is not possible | |

OPTIONAL COVER - Cyber Theft and Telephone Phreaking

- | | | |
|--|---|---|
| 1. Do you want Optional Cover for Cyber Theft and Telephone Phreaking? | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
| 2. Annual Aggregate Limit for Cyber Theft | <input type="checkbox"/> \$5,000 <input type="checkbox"/> \$10,000
<input type="checkbox"/> \$25,000 <input type="checkbox"/> \$50,000 | |
| 3. Do you require passwords be changed regularly (at least quarterly)? | <input type="checkbox"/> Yes | <input type="checkbox"/> No <input type="checkbox"/> Don't Know |
| 4. Do you allow remote access to your internal network? | <input type="checkbox"/> Yes <input type="checkbox"/> Yes, with dual authentication
<input type="checkbox"/> No <input type="checkbox"/> Don't know | |
| 5. Are all new payees, and changes to existing payees' banking details, double authenticated with the payee? | <input type="checkbox"/> Yes | <input type="checkbox"/> No <input type="checkbox"/> Don't Know |
| 6. Do transfers > \$10,000 require dual signature or supervisor / manager sign off? | <input type="checkbox"/> Yes | <input type="checkbox"/> No <input type="checkbox"/> Don't Know |
| 7. Do you provide any of the following services for others.
<i>Tick all that apply</i> | <input type="checkbox"/> Collection or payment processing?
<input type="checkbox"/> Asset, investment or trust management services?
<input type="checkbox"/> Cash management or other treasury functions?
<input type="checkbox"/> Other office functions?
<input type="checkbox"/> If 'Other', please provide details
<div style="border: 1px solid #ccc; height: 20px; width: 100%; margin-top: 5px;"></div> | |
| 8. Have you ever been declined for Crime, Fidelity or Computer Crime insurance, or had such insurance cancelled? | <input type="checkbox"/> Yes
<input type="checkbox"/> If yes, please provide details
<div style="border: 1px solid #ccc; height: 20px; width: 100%; margin-top: 5px;"></div> | <input type="checkbox"/> No
<input type="checkbox"/> N/A - have never had such insurance |
| 9. Have you ever suffered a Crime, Fidelity or Computer Crime loss? | <input type="checkbox"/> Yes
<input type="checkbox"/> If yes, please provide details
<div style="border: 1px solid #ccc; height: 20px; width: 100%; margin-top: 5px;"></div> | <input type="checkbox"/> No |

OPTIONAL COVER - Tangible Property

- | | | |
|--|--|-----------------------------|
| 1. Do you want Optional Cover for Tangible Property? | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
| 2. Annual Aggregate Limit for Tangible Property | <input type="checkbox"/> \$5,000 <input type="checkbox"/> \$10,000 <input type="checkbox"/> \$15,000 | |

Questions Below This Row Are For Risks With Revenue Of \$25 M+

EMERGENCE

<p>1. Describe the type of information in records held by you: <i>Tick all that apply</i></p>	<p><input type="checkbox"/> Customer info (e.g., Name, Address, e-mail address, Phone, etc.)</p> <p><input type="checkbox"/> Credit card details</p> <p><input type="checkbox"/> Personal Identity info (e.g., Drivers License, TFN, Passport #, Gov't ID)</p> <p><input type="checkbox"/> Banking or Financial details</p> <p><input type="checkbox"/> Medical or Healthcare data</p> <p><input type="checkbox"/> Confidential 3rd party trade secrets or IP (Intellectual Property)</p>
<p>2. Do you have a dedicated person responsible for your IT infrastructure, data security and privacy?</p>	<p><input type="checkbox"/> Yes, full time IT Manager, Chief Information Security Officer (CISO) or similar</p> <p><input type="checkbox"/> Outsourced - IT contractor provides a full time dedicated person</p> <p><input type="checkbox"/> No, responsibility is shared amongst Legal, HR and other departments</p> <p><input type="checkbox"/> No <input type="checkbox"/> Don't know</p>
<p>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?</p>	<p><input type="checkbox"/> Yes, current and tested <input type="checkbox"/> Yes, but not ever tested</p> <p><input type="checkbox"/> Yes, but not tested in last 18 months <input type="checkbox"/> No</p>
<p>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)?</p>	<p><input type="checkbox"/> Yes, multiple aspects <input type="checkbox"/> No</p> <p><input type="checkbox"/> Yes, but just one aspect</p>
<p>5. Do you control / limit / monitor your employees' ability to remove data or information from your network / office (examples include USB drive security)?</p>	<p><input type="checkbox"/> Yes, for data and physical information <input type="checkbox"/> Yes, for physical information only</p> <p><input type="checkbox"/> Yes, for data only <input type="checkbox"/> No</p>
<p>6. Does your website use Web Apps?</p>	<p><input type="checkbox"/> Yes <input type="checkbox"/> Don't Know</p> <p><input type="checkbox"/> No <input type="checkbox"/> N/A - we do not have a website</p>
<p>7. Do you use monitored Intrusion Detection or Intrusion Prevention Systems (IDS/IPS)?</p>	<p><input type="checkbox"/> Yes <input type="checkbox"/> Don't Know</p> <p><input type="checkbox"/> No</p>
<p>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?</p>	<p><input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p><input type="checkbox"/> If yes, please provide details</p> <div style="border: 1px solid black; height: 20px; width: 100%;"></div>
<p>9. Have you had any unforeseen down time to your website or IT network of more than 12 hours?</p>	<p><input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p><input type="checkbox"/> If yes, please provide details</p> <div style="border: 1px solid black; height: 20px; width: 100%;"></div>

I/we acknowledge that:

1. I/We have read and understood the important information provided at the back of the document in the important information section
2. All information given 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 form are not in my/our handwriting, I/We have checked and certify that the answers are true and correct

SIGNATURE(S) OF INSURED(S)

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:

- 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 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 something

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 us to administer and issue policies, alterations and renewals. In all aspects of arranging this policy, Emergence acts as an agent for us and not for you.

Contact details are:

Email: contractadmin@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