Cyber private enterprise
Insurance application form

CYBERNB

CAN

Basic company details

Please complete the following details for the entire company or group (including all subsidiaries) that is applying for the insurance policy:

Company Name: Primary Industry Sector:

Primary Address (Address, Province, Postal code):

Description of Business Activites:

Website Address:

Date Established (DD/MM/YYYY): Number of employees:

Last Complete Financial Year Revenue: $ Revenue From US Sales (%):

Please state which financial institution(s) you use for your commercial banking:

Primary contact details

To allow us to provide information about downloading our incident response app and receiving risk management alerts and updates, please provide contact details for the most relevant person within your organization for receiving such updates:

Contact Name: Position:

Email Address: Telephone Number:

Basic risk questions

Please confirm whether multi-factor authentication is always enabled on all email accounts: ☐ Yes ☐ No

Do you maintain daily offline back-ups of all critical data? ☐ Yes ☐ No

Is any part of your IT infrastructure outsourced to third party technology providers, including application service providers? ☐ Yes ☐ No

If you answered yes to the question above, please list your most critical third party technology providers overleaf (up to a maximum of 10).

Previous cyber incidents

Please tick all the boxes below that relate to any cyber incident that you have experienced in the last three years (there is no need to highlight events that were successfully blocked by security measures):

☐ Cyber Crime ☐ Cyber Exortion ☐ Data Loss ☐ Denial of Service Attack

☐ IP Infringement ☐ Malware Infection ☐ Privacy Breach ☐ Ransomware

☐ Other (please specify)

If you ticked any of the boxes above, did the incident(s) have a direct financial impact upon your business of more than $10,000? ☐ Yes ☐ No

If 'yes', please provide more information below, including details of the financial impact and measures taken to prevent the incident from occuring

Please list your critical third party technology providers below (up to a maximum of 10):

Revenue analysis

Please complete the answers to the questions below. Where you do not have the exact information available please provide the closest approximation and indicate that you have taken this approach.

Please provide the following details for your top 5 clients:

Client name:	Primary Services:	Annual Revenue:

IT resourcing and infrastructure

What was your approximate operational expenditure on IT security in the last financial year (including salaries, annual licenses, consultancy costs, etc.):

What was your approximate capital expenditure on IT security in the last financial year (including hardware, one off software costs, etc.):

Do you anticipate spending more, the same or less in this financial year?

Is your IT infrastructure primarily operated and managed in-house or outsourced?

How many full-time employees do you have in your IT department?

How many of these employees are dedicated to a role in IT security?

Information security governance

Who is responsible for IT security within your organisation (by job title)?

How many years have they been in this position within your company?

Please describe the type, nature and volume of the data stored on your network:

Please describe your data retention policy:

Do you comply with any internationally recognized standards for information governance (if yes, which ones):

Cyber security controls

If your organization uses Remote Desktop Protocol (RDP) to allow remote access to your network, please describe the measures you adopt to secure it:

Please describe your process for patching all operating systems and applications:

How often do you conduct vulnerability scanning of your network perimeter?

How often do you conduct penetration testing of you network architecture?

Please provide details of the third party providers you use to conduct penetration testing:

Please tick all the boxes below that relate to controls that you currently have implemented within your IT infrastructure (including where provided by a third party). If you're unsure of what any of these tools are, please refer to the explanations on the final page of this document.

☐ Advanced Endpoint Protection	☐ Application Whitelisting	☐ Asset Inventory	☐ Custom Threat Itelligence
☐ Database Encryption	☐ Data Loss Prevention	☐ DDoS Mitigation	☐ DMARC
☐ DNS Filtering	☐ Employee Awareness Training	☐ Incident Response Plan	☐ Intrusion Detection System
☐ Mobile Device Encryption	☐ Penetration Tests	☐ Perimeter Firewalls	☐ Security Info & Event Management
☐ Two-factor Authentication	☐ Vulnerability Scans	☐ Web Application Firewall	☐ Web Content Filtering

Please provide the name of the software or service provider that you use for each of the controls highlighted above:

Important notice

By signing this form you agree that the information provided is both accurate and complete and that you have made all reasonable attempts to ensure this is the case by asking the appropriate people within your business. CFC Underwriting will use this information solely for the purposes of providing insurance services and may share your data with third parties in order to do this. We may also use anonymized elements of your data for the analysis of industry trends and to provide benchmarking data. For full details on our privacy policy please visit ***www.cfcunderwriting.com/privacy***

Contact name: Position:

Signature: Date (DD/MM/YYYY):