Cyber Enterprise Risk Management Insurance

Short Proposal Form

CHUBB®

Important Notices

Statement pursuant to Section 25 (5) of the Insurance Act (Cap. 142) (or any subsequent amendments thereof) - You are to disclose in this Proposal Form fully and faithfully all facts which you know or ought to know, otherwise the policy issued hereunder may be void.

Your Duty of Disclosure
Before you enter into a contract of general insurance with an insurer, you have a duty under the law to disclose to the insurer every matter within your knowledge that is material to the insurer's decision whether to accept the risk of the insurance and, if so, on what terms. If you are unsure whether a matter is material, you should disclose it. You have the same duty to disclose those matters to the insurer before you renew, extend, vary or reinstate a contract of general insurance.

It is important that all information contained in this application is understood by you and is correct, as you will be bound by your answers and by the information provided by you in this application. You should obtain advice before you sign this application if you do not properly understand any part of it. Your duty of disclosure continues after the application has been completed up until the contract of insurance is entered into.

Non-Disclosure
If you fail to comply with your duty of disclosure, the insurer may have the option of avoiding the contract of insurance from its beginning. If your non-disclosure is fraudulent, the insurer may also have the right to keep the premium that you have paid.

Change of Risk or Circumstances
You should advise the insurer as soon as practicable of any change to your normal business as disclosed in this application, such as changes in business activities, location, acquisitions and new overseas activities.

Subrogation
Where you have agreed with another person or company (who would otherwise be liable to compensate you for any loss or damage which is covered by the contract of insurance) that you will not seek to recover such loss or damage from that person, the insurer will not cover you, to the extent permitted by law, for such loss or damage.

This document allows Chubb to gather the needed information to assess the risks related to the information systems of the prospective insured. Please note that completing this short proposal form does not bind Chubb, or the prospective insured, to conclude an insurance policy. If the Information Systems Security Policy of the companies/subsidiaries of the prospective insureds varies, please complete the proposal form for each prospective insured. Please also note that further information, including a full proposal form, may be required.

Company Information

Company Name:

Company Website:

Address: Postal Code

Please provide contact details for the client's CISO or other staff member who is responsible for data and network security:

Name (First and Surname): Role:

Email: Phone:

Annual Turnover (S$):

Percentage of turnover generated from:

SG	Australia	USA / Canada	Asia	Europe (EU)	Rest of the World

Profile of the Company / Companies to be Insured

What is the Insured's Business Description?

Is your business a subsidiary, franchisee, or smaller entity of a larger organisation? ☐ Yes ☐ No

Do you provide ANY services to, or trade with individuals or organisations in sanctioned territories including but not limited to Iran, Syria, North Sudan, Crimea Region, and Cuba, or any territory that is subject to certain US, EU, UN, and/or other national sanctions restrictions? ☐ Yes ☐ No

Do you currently, or will you potentially operate as any of the following? *(Select all that applies)* ☐ Yes ☐ No

- ☐ Accreditation Services
- ☐ Adult Content Services
- ☐ Credit Bureau
- ☐ Cryptocurrency Exchange or Distributed Ledger Technology
- ☐ Cybersecurity Products or Services
- ☐ Data Aggregation / Brokerage / Warehousing
- ☐ Financial Institution
- ☐ Gambling Industry
- ☐ IT Managed Service Provider
- ☐ Local or regional authority
- ☐ Manufacturer of Life Safety Products or Services
- ☐ Media Production
- ☐ Payment Processing or Trading Exchanges
- ☐ Peer to Peer File Sharing
- ☐ Social Media Platform
- ☐ Surveillance (Physical or Digital)
- ☐ Third Party Claims Administration

Additional commentary on business operations:

Qualifying Questions

1. Does any part of your network (including email) maintain remote access capability? ☐ Yes ☐ No

   a. If yes, is Multi-Factor Authentication required for all remote network access capability? ☐ Yes ☐ No

   Commentary:

2. Does the possible maximum number of individuals you would be required to notify in case of a breach of Personally Identifiable Information (PII) exceeds 500,000? ☐ Yes ☐ No

   Commentary:

3. To the best of your knowledge, does your business comply with all relevant Privacy Laws and Regulations in the jurisdictions in which you operate? ☐ Yes ☐ No

   Commentary:

4. Do you or your outsourced service provider, accept payment card transactions? ☐ Yes ☐ No

   a. If yes, are you compliant to the level of PCI DSS that applies to your company? ☐ Yes ☐ No

   Commentary:

5. Please confirm your backups for mission critical systems are protected by the following *(select all that apply)*:

   ☐ immutable or Write Once Read Many (WORM) protections
   ☐ completely Offline or Air-gapped Segmentation from the rest of your network
   ☐ access to backups is restricted via separate Privileged Accounts that are not connected to your standard Active Directory Domain
   ☐ access to backups is restricted via Multi-Factor Authentication
   ☐ none of the protections listed

   Commentary:

6. Please confirm which of the following endpoint protection technologies are in place on all laptops, desktops, and servers *(select all that apply)*:

   ☐ advanced or next-generation anti-malware and anti-virus with Heuristic Analysis
   ☐ URL filtering or Web Filtering
   ☐ application isolation and containment technologies
   ☐ Centralized Endpoint Protection Platform

☐ EDR (endpoint detection and response), XDR (extended detection and response), or MDR (managed detection and response)
☐ none of the protections listed

Commentary:

7. Please confirm which of the following email security measures are in place *(select all that apply)*:

☐ quarantine service for suspicious emails
☐ ability to detonate attachments and links in a Sandbox
☐ Sender Policy Framework (SPF) is enforced
☐ Microsoft Office macros are disabled on documents by default
☐ phishing simulations or other training for employees on at least an annual basis
☐ none of the protections listed

Commentary:

8. Within the last 3 years, has your business had any Cyber Incidents, Data Breaches, privacy complaints, or become aware of any matter that could lead to a claim under a cyber insurance policy? ☐ Yes ☐ No

Commentary:

I/we declare that I/we have made a fair presentation of the risk, by disclosing all material matters which I/we know or ought to know or, failing that, by giving the Insurer sufficient information to put a prudent insurer on notice that it needs to make further enquiries in order to reveal material circumstances.

Signatory Name and Surname	Function
Date	Signature

Glossary of Terms

Active Directory Domain – An Active Directory domain is a collection of objects within a Microsoft Active Directory network. An object can be a single user or a group, or it can be a hardware component, such as a computer or printer. Each domain holds a database containing object identity information.

Advanced Endpoint Protection – Advanced Endpoint Protection is a device or software that provides protects and monitors the endpoints on your network. Endpoints include desktop and laptop computers, tablets, mobile phones, servers, and any other device connected to your network

- **EDR (endpoint detection and response) –** is a solution which records and stores endpoint-system-level behaviors, use various data analytics techniques to detect suspicious system behavior, provide contextual information, block malicious activity, and provide remediation suggestions to restore affected systems.

- **MDR (managed detection and response) –** is a managed cyber security service that provides intrusion detection of malware and malicious activity in your network, and assists in rapid incident response to eliminate those threats with succinct remediation actions.

- **XDR (extended detection and response) –** is a security threat detection and incident response tool that natively integrates multiple security products into a cohesive security operations system that unifies all licensed components, typically including endpoints, networks, servers, cloud services, SIEM, and more.

Application Isolation & Containment – this technology can block, restrict, or isolate specific endpoints from performing potentially harmful actions between endpoints and other applications or resources with the goal to limit the impact of a compromised system or endpoint.

Centralised Endpoint Protection Platform – is a solution deployed on endpoint devices to prevent file-based malware attacks, detect malicious activity, and provide the investigation and remediation capabilities needed to respond to dynamic security incidents and alerts.

Cyber Incident – includes unauthorised access to your computer systems, hacking, malware, virus, ransomware, distributed denial of service attack, insider misuse, human or programming error, system outage, or any other cyber-related event.

Data Breach – means an incident where sensitive personal or corporate confidential information has been taken, lost, or viewed by an unauthorised party.

Heuristic Analysis – going beyond traditional signature-based detection in basic antivirus software, heuristic analysis looks for suspicious properties in code, and can determine the susceptibility of a system towards particular threat using various decision rules or weighing methods designed to detect previously unknown computer viruses, as well as new variants of viruses already in the "wild".

Multi-Factor Authentication (MFA) – MFA is an electronic authentication method used to ensure only authorised individuals have access to specific systems or data. A user is required to present two or more factors – these factors being 1) **something you know**, 2) **something you have**, or 3) **something you are**.
Something you know may include your password or a pin code.
Something you have may include a physical device such as a laptop, mobile device that generates a unique code or receives a voice call or a text message, a security token (USB stick or hardware token), or a unique certificate or token on another device. **Something you are** may include biometric identifiers.

- Note that the following are <u>not</u> acceptable second factors: a shared secret key, an IP or MAC address, a VPN, a monthly re-authentication procedure, or VOIP authentication.

Offline or Air-gapped Segmentation – as it relates to backup solutions, offline or air-gapped storage means that a copy of your data and configurations are stored in a disconnected environment that is separate to the rest of your network. Physical tape or non-mounted disk backups that aren't connected to the internet or LAN would be considered offline.

PCI DSS – PCI DSS stands for the Payment Card Industry Data Security Standard. This defines the requirements that a company must comply with if they handle any payment card information or accept payment card transactions.

Privacy Laws and Regulations – The body of law that sets the requirements and regulations for the collection, storage, and usage of personally identifiable information, personal healthcare information, financial information of individuals, and other sensitive data which may be collected by public or private organisations, or other individuals.

Sandbox – as it relates to email solutions, a sandbox filters emails with unknown URL links, attachments, or other files, allowing them to be tested in a separate and safe environment before allowing them to proceed to your network or mail servers.

Sender Policy Framework (SPF) – is an email authentication method that is used to prevent unauthorised individuals from sending email messages from your domain, and generally helps to protect email users and recipients from spam and other potentially dangerous emails.

Personally Identifiable Information (PII) – means any data that can be used to identify a specific individual. This may include health or medical records of employees or customers, government issued identification numbers, login usernames, email addresses, credit card numbers, biometric information, and other related personal information.

Privileged Accounts – means accounts that provide administrative or specialised levels of access based on a higher level of permission.

URL Filtering or Web Filtering – is technology that restricts which websites a user or browser can visit on their computer, typically filtering out known malicious or vulnerable websites.

Write Once Read Many – a data storage device in which information, once written, cannot be modified.

Data Protection Notice

Chubb Insurance Singapore Limited ("Chubb") is committed to protecting your personal data. Chubb collects, uses, discloses and retains your personal data in accordance with the Personal Data Protection Act 2012 and our own policies and procedures. Our Personal Data Protection Policy is available upon request. Chubb collects your personal data (which may include health information) when you apply for, change or renew an insurance policy with us, or when we process a claim. We collect your personal data to assess your application for insurance, to provide you with competitive insurance products and services and administer them, and to handle any claim that may be made under a policy. If you do not provide us with your personal data, then we may not be able to provide you with insurance products or services or respond to a claim.

We may disclose the personal data we collect to third parties for and in connection with such purposes, including contractors and contracted service providers engaged by us to deliver our services or carry out certain business activities on our behalf (such as actuaries, loss adjusters, claims investigators, claims handlers, third party administrators, call centres and professional advisors, including doctors and other medical service providers), other companies within the Chubb Group, other insurers, our reinsurers, and government agencies (where we are required to by law). These third parties may be located outside of Singapore.

You consent to us using and disclosing your personal data as set out above. This consent remains valid until you alter or revoke it by providing written notice to Chubb's Data Protection Officer ("DPO") (contact details provided below). If you withdraw your consent, then we may not be able to provide you with insurance products or services or respond to a claim.

From time to time, we may use your personal data to send you offers or information regarding our products and services that may be of interest to you. If you do not wish to receive such information, please provide written notice to Chubb's DPO.

If you would like to obtain a copy of Chubb's Personal Data Protection Policy, access a copy of your personal data, correct or update your personal data, or have a complaint or want more information about how Chubb manages your personal data, please contact Chubb's DPO at:

Chubb Data Protection Officer
Chubb Insurance Singapore Limited
138 Market Street
#11-01 CapitaGreen
Singapore 048946
E dpo.sg@chubb.com

Contact Us

Chubb Insurance Singapore Limited
Co Regn. No.: 199702449H
138 Market Street
#11-01 CapitaGreen
Singapore 048946
O +65 6398 8000
E FinancialLines.SG@chubb.com
www.chubb.com/sg

Chubb. Insured.™

Published 04/2022.