

Options & Pricing

Coverage Limit Revenue	\$500,000	\$1M	\$2M	\$3M	Deductible
< \$1M	\$1,690	\$1,885	\$2,340	\$3,075	\$1,500
< \$2.5M	\$2,145	\$2,340	\$2,925	\$4,648	\$2,500
< \$5M	\$2,730	\$3,003	\$3,835	\$6,149	\$3,500
< \$10M	\$3,822	\$4,225	\$5,265	\$7,865	\$5,000
< \$20M	\$6,440	\$7,520	\$9,120	\$12,848	\$10,000
< \$35M	\$7,920	\$9,120	\$11,520	\$14,520	\$12,500
< \$50M	\$10,320	\$11,120	\$13,920	\$18,040	\$15,000

Premiums indicated are in Singapore dollars and excludes GST, which is payable in addition.
A deductible (waiting period) of 12 hours applies following a business interruption incident.

PARTICULARS OF COMPANY ("INSURED")

Name of Company ("Insured"):

Company Registration No.:

Nature of Business:

Revenue for the last 12 months: S\$

Registered Address:

Mailing Address:

Contact Person:

Contact No: Email:

INCEPTION OF POLICY

12 months effective from: / /

DECLARATION

The undersigned authorised officers of the Applicant declare that to the best of their knowledge and belief the statements set forth herein and all attachments and schedules hereto are true and immediate notice will be given should any of the above information alter between the date of this proposal and the proposed date of inception of the insurance. Although the signing of the proposal does not bind the undersigned, on behalf of the Applicant, to effect insurance, the undersigned agree that this proposal and all attachments and schedules hereto and the said statements herein shall be the basis of and will be incorporated in the policy should one be issued. The undersigned, on behalf of the Applicant, acknowledge that the Statutory Notice contained herein has been read and understood. This proposal must be signed by the Applicant's Chairman of the Board, Managing Director or Chief Executive Director.

PERSONAL INFORMATION COLLECTION STATEMENT

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

Name & Signature of Chairman, Managing director or Chief Executive Director

Date

Cyber Enterprise Risk Management is underwritten by Chubb Insurance Singapore Limited ("Chubb") and distributed by DBS Bank Ltd ("DBS"). Full details of the terms, conditions and exclusions of the insurance are provided in the policy wordings and will be sent to you upon acceptance of your application by Chubb.



Cyber Enterprise Risk Management

Mitigate against your business's cyber risks

In today's connected environment, cyber security is a widespread concern. All too often, businesses do not fully understand their organisation's cyber and data privacy risks until an event occurs. Any company can be affected by a breach of sensitive customer or employee information. Even the loss of a single laptop, if not properly managed, can turn into a public relations disaster.

Chubb understands that small businesses are all the more vulnerable to such risks and will need adequate protection for their growing business. With Chubb's worldwide experience and capability, coupled with local underwriting and risk management expertise across Asia, Chubb can help you move your business forward with confidence.

Key Coverages



Business Interruption and Data Recovery

Loss of profits, as well as recovery expenses due to a network security failure or attack, human errors, or programming errors.



Incident Response

Forensic IT services; Crisis communications and reputational mitigation; Legal advice and investigation costs, supported by incident reporting hotline and local vendor.



Third Party Claims

Legal liability resulting from cybersecurity breaches, including failure to maintain confidentiality of data, payment for fines and penalties. Regulatory investigations or enforcement proceedings expenses will also be covered.



Network or Data Extortion / Blackmail



Worldwide Cover

Value-Added Services from Chubb

- 24/7/365 day incident response hotline
- Specialist vendor panel with local, regional and global capabilities
- Self-help web portal called the eRisk Hub
- Empowered local underwriters
- The Chubb claims commitment

Loss Scenarios

1. EMPLOYEE ACCESSES HR SITE AND SELLS PERSONAL INFORMATION

Cause of action - Negligence and Invasion of Privacy

Coverage triggers - Incident Response Expenses and Data Asset Loss

Type of organisation - Professional Services Firm

Number of employees - 25

Annual revenue - S\$7.5 million

Description of event - A rogue employee accessed the human resource platform of a professional service provider. The employee acquired and sold social security information on the black market before being apprehended by law enforcement. Thereafter, several cases of identity theft were perpetrated against the professional service provider's employees.

Resolution - The professional service provider engaged a forensics investigator and outside compliance counsel. It also notified employees of the breach, established a call centre, and provided monitoring and restoration services to impacted employees.

Total costs incurred from the event - S\$75,000

2. EMPLOYEE BREACHES INTERNAL GOVERNANCE

Cause of action - Negligence, Procedure Breach leading to Business Interruption

Coverage triggers - Business Interruption, Data Asset Loss, Recovery Costs, Incident Response Expense

Type of organisation - Retail Store

Number of employees - 20

Annual revenue - S\$5 million

Description of event - An employee at a hardware store ignored internal policies and procedures and opened a seemingly innocuous file attached to an email. The next day the hardware store's stock order and cash registers started to malfunction and business trade was impaired as a result of the network failure.

Resolution - The hardware store incurred over S\$100,000 in forensic investigation and restoration services. They also had additional increased working costs of S\$20,000 and business income loss estimated at S\$50,000 from the impaired operations.

Total costs incurred from the event - S\$170,000

CHUBB®

Chubb Insurance Singapore Limited
Co. Reg No. 199702449H
138 Market Street, #11-01 CapitaGreen, Singapore 048946
CS +65 6398 9797 F +65 6298 1055
www.chubb.com/sg

Cyber Enterprise Risk Management Enrolment Form

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.

UNDERWRITING CRITERIA

This product offers companies with gross revenue of below S\$50 million up to S\$2 million limit coverage.

Excluded Industries

- Adult Content Sites
- Credit Bureaus
- Credit Card Processor
- Data Aggregators
- Data Processors (BPO's)
- Financial Institutions, Security and Commodity Brokers
- Hospitals
- Online Exchanges, Stock Exchanges, Virtual Currency Exchanges
- Payment Gateways
- Social Networking Sites
- Telecommunications, Internet Service Providers, Application Service Providers, Cloud providers, Search Engine Providers
- Universities
- Utilities (Water, Electricity, Energy etc) including Critical Infrastructure

The Insured and all subsidiaries:

- Have no more than 20% of annual revenue generated from USA and/or Canada.
- Comply with the Payment Card Industry (PCI) Standards and if not compliant, do not process more than 1 million debit/credit card transactions in the last 12 months.
- Have up-to-date antivirus and firewall protection software installed and operating on all computers systems.
- Have software installed that is authorised and/or commercially licensed and updated (patches, upgrades) when necessary.
- Conduct backup and recovery procedures on all sensitive and financial data on at least a weekly basis.
- Have encryption policies or password security measures for all mobile devices (including laptops and USB sticks).
- Comply with privacy and data protection legislation applicable to all jurisdictions and industry standards, in which it operates.
- Have not ever given notice under the provisions of any prior or current cyber policy or similar insurance and is not aware of any incident which might give rise to a claim. Incidents include any unauthorised access to any computer, computer system, database, intrusion or attacks, denial of use of any computer or system, intentional disruption, corruption, or destruction of data, programs, or applications, any cyber extortion event(s); or any other incidents similar to the foregoing including those that have resulted in a claim, administrative action, or regulatory proceeding.