



Proposal Form

CYBER SECURITY INSURANCE

This is a Proposal Form for a loss/claims-discovered Policy. Said Policy is subject to terms & conditions and coverage is limited to losses and claims first discovered during the period of insurance or any discovery period, if applicable.

Please note, completion and signing of this document does not bind either party to enter into a contract of insurance. However, when filling out this Proposal Form, do provide accurate, complete and honest information. Failure to do so may affect the right to cover should a Policy be issued.

Herein, unless otherwise specified,

- the term “Company” refers to the Proposer and all its subsidiaries. If the responses for any subsidiary differ from those provided by the Proposer, please provide these on a separate signed sheet.
- the term “Employee” refers to any natural person who is under any express or constructive contract of employment (whether full time, part-time or temporary) with the Company.

Should the space left for answering be insufficient, please use a separate signed sheet.

Information & Activities

1. Please provide the following details:

Company name (including any trading names):

Corporate Headquarter:

Five biggest locations (revenue-wise):

Number of employees:

Date of establishment:

Website address:

2. Please write a brief description of your Company activity in the space provided below:

3. Consolidated Financial Overview:

Latest Complete Financial Year in Currency:

Gross Annual Revenue:

Annual Net Income Before Taxes:

Revenue Arising from Online Activities:

4. Please estimate the percentage split of your turnover by regions:

Work carried out for:	Last Year
Domestic clients:	<input type="text"/> %
European clients:	<input type="text"/> %
US/Canadian clients:	<input type="text"/> %
Asian-Pacific clients:	<input type="text"/> %
Other clients:	<input type="text"/> %

General Risk-related Information

5. What is the estimated total number of records, including employees and customers, that your Company holds:

6. Type of Record:

	(yes)	If yes , please provide estimated no. of records:	(no)
Personally Identifiable Information (PII)*	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>
Other Personal Information (Religion, Gender...)	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>
Protected Health Information (PHI)**	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>
Debit/Credit Card Numbers	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>
Financial Information	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>
Social Security Numbers	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>
Drivers Licence Numbers	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>
Other type of information	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>

*Information that can be used to uniquely identify, contact or locate a single person, or can be used with other sources to uniquely identify a single individual.

**Any information about health status, provision of health care, or payment for health care that can be linked to a specific individual.

7. Do you process or store any type of records on behalf of third parties? (yes) (no)

If **yes**, please explain:

8. Do you allow your staff to use personal devices for work related purposes? (yes) (no)

 If **yes**, have you set up a Bring Your Own Device (BYOD) policy? (yes) (no)

Risk-related Declarations

This section is broken down into the following three subsections:

- **PEOPLE** (Governance, Compliance, Human Resources...)
- **PROCESSES** (Policies & Procedures...)
- **TECHNOLOGY** (Budget, Information Technology...)

These are the three pillars upon which we can assess Security and Cyber Resilience within your organisation.

PEOPLE

9. Please answer, regarding **Human Resources** at your Company:

	(yes)	(no)
a) Do you have a Chief Privacy Officer (CPO), Data Protection Officer (DPO) or Chief Compliance Officer who is assigned responsibility for your global obligations under Data Protection and Privacy legislations?	<input type="checkbox"/>	<input type="checkbox"/>
b) Do you have an information security team (IST)?	<input type="checkbox"/>	<input type="checkbox"/>
If yes , is the IST managed from a central location and has local relays in each region where your Company operates?	<input type="checkbox"/>	<input type="checkbox"/>



- | | | |
|---|--------------------------|--------------------------|
| | (yes) | (no) |
| c) Does your organization offer Privacy Awareness Training / other Cyber-related trainings? | <input type="checkbox"/> | <input type="checkbox"/> |
| d) Does your hiring process for employees require, when authorised by law, a full background check including Criminal, Educational, and Credit? | <input type="checkbox"/> | <input type="checkbox"/> |

10. Please answer, regarding **Vendor & Third-Party Management** at your Company:

- | | (yes) | (no) | | | | | | | | | | | | |
|---|--------------------------|--------------------------|--|--|--|--|--|--|--|--|--|--|--|--|
| a) Do you outsource any portion of your information security and/or data processing?
If yes , please provide us with the name(s) of the provider(s) and the service(s) being provided. | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | | | | | | | |
| <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 50%;">Provider(s):</th> <th style="width: 50%;">Service(s):</th> </tr> </thead> <tbody> <tr><td style="height: 15px;"> </td><td style="height: 15px;"> </td></tr> <tr><td style="height: 15px;"> </td><td style="height: 15px;"> </td></tr> <tr><td style="height: 15px;"> </td><td style="height: 15px;"> </td></tr> <tr><td style="height: 15px;"> </td><td style="height: 15px;"> </td></tr> <tr><td style="height: 15px;"> </td><td style="height: 15px;"> </td></tr> </tbody> </table> | Provider(s): | Service(s): | | | | | | | | | | | | |
| Provider(s): | Service(s): | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| b) Do all third party contracts include the following security provisions? | | | | | | | | | | | | | | |
| A service level agreement that specifies security requirements and responsibilities | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | | | | | | | |
| Provisions for compliance with applicable regulations (SOX, HIPAA, PCI...) | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | | | | | | | |
| A right-to-audit clause | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | | | | | | | |
| Procedures for escalating security related events | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | | | | | | | |
| If any of the above responses are no , please explain: | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| c) Do you require providers to indemnify you in case of any data breach? | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | | | | | | | |
| d) Do you require providers to have their own data protection liability insurance coverage? | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | | | | | | | |

11. Please answer, regarding **Audit & Compliance** at your Company:

- | | | |
|--|---|--------------------------|
| | (yes) | (no) |
| a) Do you have a programme in place to periodically test IT security controls?
(This can include internal audits, external audits or security consulting engagements.) | <input type="checkbox"/> | <input type="checkbox"/> |
| If yes , do these controls include (please mark if applicable): | | |
| Outside security specialists performing penetration testing | <input type="checkbox"/> | |
| Automated vulnerability scanners | <input type="checkbox"/> | |
| Secure configuration checkers | <input type="checkbox"/> | |
| Performance tools | <input type="checkbox"/> | |
| Source code comparison tools | <input type="checkbox"/> | |
| Security policies and controls being subject to independent reviews and audits | <input type="checkbox"/> | |
| b) Are critical and high-risk vulnerabilities remediated within one month? | <input type="checkbox"/> | <input type="checkbox"/> |
| c) Do you comply with privacy and data protection legislation applicable to all jurisdictions and industry standards in which you operate?
(e.g. Australian Privacy Principles, HIPAA privacy Rules, GDPR...) | <input type="checkbox"/> | <input type="checkbox"/> |
| d) Is your Company subject to Payment Card Industry (PCI) Security Standards? | <input type="checkbox"/> | <input type="checkbox"/> |
| If yes , what level of requirement? | <input type="checkbox"/> 1 / <input type="checkbox"/> 2 / <input type="checkbox"/> 3 / <input type="checkbox"/> 4 | |
| e) When acquiring a new company is specific IT Due Diligence undertaken? | <input type="checkbox"/> | <input type="checkbox"/> |
| If yes , is the IT system of the acquired company screened prior to acquisition? | <input type="checkbox"/> | <input type="checkbox"/> |



PROCESSES

12. Please answer, regarding **Risk Mapping and Information Security** at your Company:

	(yes)	(no)
a) Have you implemented a Data & System Classification policy with specific rules that apply to each classification level?	<input type="checkbox"/>	<input type="checkbox"/>
b) Have you performed an inventory of critical business information in the last 24 months?	<input type="checkbox"/>	<input type="checkbox"/>

13. Please answer, regarding the **Information Security Policy** at your Company:

	(yes)	(no)
a) Do you have a formal Information Security Policy implemented corporate-wide and applicable to all business units?	<input type="checkbox"/>	<input type="checkbox"/>
If yes , do you (please mark if applicable):		
Make the Policy permanently available for employees, contractors and concerned parties?	<input type="checkbox"/>	
Test the security required by the security policy at least once, annually?	<input type="checkbox"/>	
Regularly identify, assess new threats and adjust the security policy accordingly?	<input type="checkbox"/>	
Include Internet Usage, Acceptable Use and Email Use in the Policy?	<input type="checkbox"/>	
Include use and storage of information on laptops in the Policy?	<input type="checkbox"/>	
Share the Policy with contractors and external consultants?	<input type="checkbox"/>	
If yes , when was the last time the Policy was reviewed and / or updated?	<input style="width: 50px;" type="text"/>	

14. Please answer, regarding the **Password Policy, Logs review & Patch Management** at your Company:

	(yes)	(no)
a) Do you enforce a password management policy?	<input type="checkbox"/>	<input type="checkbox"/>
If yes , how often are passwords required to be changed?		
< 90 days	<input type="checkbox"/>	
< 180 days	<input type="checkbox"/>	
Annually	<input type="checkbox"/>	
Other	<input style="width: 50px;" type="text"/>	
And, if yes , is password complexity defined and made mandatory?	<input type="checkbox"/>	<input type="checkbox"/>
b) Does your Company enforce a patch management process?	<input type="checkbox"/>	<input type="checkbox"/>
c) Once security patches are identified, do you prioritize based on a severity & likelihood analysis?	<input type="checkbox"/>	<input type="checkbox"/>
d) Are vulnerabilities and exploits monitored on a daily basis by a Security Operations Centre (SOC) or are you subscribed to a Managed Security Service Provider (MSSP)?	<input type="checkbox"/>	<input type="checkbox"/>

15. Please answer, regarding **Physical Security** at your Company:

	(yes)	(no)
a) Has a security perimeter been identified and documented (including computer rooms, media storage rooms, data-centres, etc.)?	<input type="checkbox"/>	<input type="checkbox"/>
b) Which of the following security controls have been implemented within your organisation? (please mark if applicable):		
Biometric Access Controls to access Company Data Centre(s)	<input type="checkbox"/>	
ID badges for employee, visitor and vendor access	<input type="checkbox"/>	
Surveillance cameras and guards monitoring premises	<input type="checkbox"/>	
Data Centre access logs monitored periodically	<input type="checkbox"/>	
Smart cards used for physical security	<input type="checkbox"/>	
Physical security management centralized for all locations	<input type="checkbox"/>	
Computer, media storage and telecom room access, secured and restricted to authorized personnel	<input type="checkbox"/>	
Cables and network ports protected from unauthorized access	<input type="checkbox"/>	



16. Please answer, regarding **Disposal** at your Company:

	(yes)	(no)
a) Do you shred all written or printed personally identifiable or other confidential information when it is being discarded?	<input type="checkbox"/>	<input type="checkbox"/>
b) Is disposal of computer systems and media storage devices (hard drives, tapes, CDs, etc.) handled in a secure way (e.g. de-magnetization, multiple wipes, deletion beyond reconstitution)?	<input type="checkbox"/>	<input type="checkbox"/>

17. Please answer, regarding **Computer & Network Management** at your Company:

	(yes)	(no)
a) Is separation of duties enforced in all critical process steps for all sensitive operations?	<input type="checkbox"/>	<input type="checkbox"/>
b) Do you have a virus protection program in place that is installed and enabled on servers, workstations and laptops?	<input type="checkbox"/>	<input type="checkbox"/>
c) To verify the security of your network perimeter, do you conduct comprehensive penetration tests?	<input type="checkbox"/>	<input type="checkbox"/>
If yes (please mark if appropriate):		
Is physical penetration tested?	<input type="checkbox"/>	
Are those tests performed by external service providers in some instances?	<input type="checkbox"/>	
If yes , how many times a year are penetration tests conducted?	<input type="text"/>	
d) Are critical applications residing within internal networks (and behind the firewall) monitored 24/7 for security violations?	<input type="checkbox"/>	<input type="checkbox"/>
e) Do critical systems receive full security testing before deployment?	<input type="checkbox"/>	<input type="checkbox"/>

18. Please answer, regarding **Change Management** at your Company:

	(yes)	(no)
a) When a new IT system is developed or purchased, are security considerations taken into account?	<input type="checkbox"/>	<input type="checkbox"/>
b) Are staging, test and development systems kept separate from production systems?	<input type="checkbox"/>	<input type="checkbox"/>
If yes , does that include (please mark if applicable):		
Use of sandboxes?	<input type="checkbox"/>	
No sharing of databases and configuration files?	<input type="checkbox"/>	
No sharing of accounts?	<input type="checkbox"/>	
No access to production for developers?	<input type="checkbox"/>	

TECHNOLOGY

19. What is your annual aggregate **IT Budget**?

Prior Year	Current Year
<input type="text"/>	<input type="text"/>

20. Please answer, regarding **IT Devices** at your Company:

a) How many data centres do you have?	<input type="text"/>
b) Where are they located?	<input type="text"/>
c) How many individual IT devices (e.g. server, desktops, laptops, mobile devices) do you deploy?	<input type="text"/>



21. Please answer, regarding **Network** at your Company:

	(yes)	(no)
a) Are firewalls used to prevent unauthorized access on all connections from internal networks and systems to external networks such as vendor's systems or the internet?	<input type="checkbox"/>	<input type="checkbox"/>
b) Are remote users authenticated before being allowed to connect to internal networks and systems?	<input type="checkbox"/>	<input type="checkbox"/>
If yes , what tools have been set up? (VPN types and VPN protocols, etc.)		
c) Is there encryption for:		
Data at rest	<input type="checkbox"/>	<input type="checkbox"/>
Data in transit	<input type="checkbox"/>	<input type="checkbox"/>
Network (network level encryption)	<input type="checkbox"/>	<input type="checkbox"/>
Endpoint devices (Laptops, tablets and removable media)	<input type="checkbox"/>	<input type="checkbox"/>
d) Do you use anti-virus, anti-spyware or an equivalent malware protection?	<input type="checkbox"/>	<input type="checkbox"/>
If yes , are virus signature files downloaded and updated automatically?		
	<input type="checkbox"/>	<input type="checkbox"/>
e) Do you use Honeypots or similar techniques to detect and deflect attempts of unauthorised use of Company Information Systems?	<input type="checkbox"/>	<input type="checkbox"/>
f) Are your networks and systems segregated as opposed to all residing on a flat network?	<input type="checkbox"/>	<input type="checkbox"/>

Cyber Incident Readiness

	(yes)	(no)
22. Are designated employees trained to obtain and handle forensic evidence, involve law enforcement and handle press relations in response to a suspected intrusion?	<input type="checkbox"/>	<input type="checkbox"/>
23. Do you have an Incident Management Programme in place that includes cyber related incidents?	<input type="checkbox"/>	<input type="checkbox"/>
If yes , is it:		
Formally documented?	<input type="checkbox"/>	<input type="checkbox"/>
Tested annually to ensure its effectiveness?	<input type="checkbox"/>	<input type="checkbox"/>
Performed by trained personnel?	<input type="checkbox"/>	<input type="checkbox"/>
25. Do you have a Business Continuity Plan (BCP) in place that includes cyber related incidents?	<input type="checkbox"/>	<input type="checkbox"/>
If yes , is it:		
Managed by a dedicated group?	<input type="checkbox"/>	<input type="checkbox"/>
Formally documented?	<input type="checkbox"/>	<input type="checkbox"/>
Tested annually to ensure its effectiveness?	<input type="checkbox"/>	<input type="checkbox"/>
Performed by trained personnel?	<input type="checkbox"/>	<input type="checkbox"/>
If yes , does it include the use of:		
Redundant systems and multiple Data Centres?	<input type="checkbox"/>	<input type="checkbox"/>
A defined "hot site"?	<input type="checkbox"/>	<input type="checkbox"/>
26. How frequently do you back up electronic data?	<input type="checkbox"/>	
27. Where do you store back-up electronic data?	<input type="checkbox"/>	



- | | (yes) | (no) |
|---|--------------------------|--------------------------|
| 28. Do you store back-up electronic data with a third-party service provider? | <input type="checkbox"/> | <input type="checkbox"/> |
| 29. Do you regularly ensure that data backups can be restored as quickly as possible with minimal impact? | <input type="checkbox"/> | <input type="checkbox"/> |
| 30. Please indicate the acceptable time for business interruption to last until a financial loss with a significant impact on your business materializes? | <input type="checkbox"/> | <input type="checkbox"/> |

Historical Information

- | | (yes) | (no) |
|--|--------------------------|--------------------------|
| 31. Are you aware of any personal or corporate data breach, cyber event (including but not limited to DDoS attacks, IT network disruption or suspension, malicious code transmission, hack) occurring at and/or spread from your IT systems or outsourced IT systems and for which a third party (including but not limited to clients, customers, data subjects or employees) might hold you responsible? | <input type="checkbox"/> | <input type="checkbox"/> |

If **yes**, please explain:

- | | | |
|---|--------------------------|--------------------------|
| 32. During the past three years: | | |
| a) Have you experienced an interruption or suspension of your computer systems for any reason (not including downtime for planned maintenance), which exceeded 4 hours? | <input type="checkbox"/> | <input type="checkbox"/> |
| b) Has any customer or other person or entity alleged that their personal data has been compromised by you or any service provider processing, handling or collecting personal data on your behalf? | <input type="checkbox"/> | <input type="checkbox"/> |
| c) Have you ever notified any person that their information was or may have been compromised? | <input type="checkbox"/> | <input type="checkbox"/> |
| d) Has your organization been subject to an investigation by a data protection authority? | <input type="checkbox"/> | <input type="checkbox"/> |

If **yes**, please explain:

- | | | |
|--|--------------------------|--------------------------|
| 33. Have you ever sustained an intentional breach of IT security, network damage, system corruption or loss of data? | <input type="checkbox"/> | <input type="checkbox"/> |
|--|--------------------------|--------------------------|

If **yes**, please explain:

Data Protection and Privacy Policy:

The insurer respects the insureds' right to privacy. In our Privacy Policy (available at <https://www.tmhcc.com/en/legal/privacy-policy>) we explain who we are, how we collect, share and use personal information about the insureds, and how the insureds can exercise their privacy rights. If the insureds have any questions or concerns about our use of their personal information, they can contact dpo-tmelux@tmhcc.com.

We may collect personal information such as name, email address, postal address, telephone number, gender and date of birth. We need the personal information to enter into and perform the current contract of insurance. We retain personal information we collect from the insureds where we have an ongoing legitimate business need to do so.

We may disclose the insureds' personal information to:

- our group companies;
- third party services providers and partners who provide data processing services to us or who otherwise process personal information for purposes that are described in our Privacy Policy or notified to the insureds when we collect their personal information;
- any competent law enforcement body, regulatory, government agency, court or other third party where we believe disclosure is necessary (i) as a matter of applicable law or regulation, (ii) to exercise, establish or defend our legal rights, or (iii) to protect the interests of our insureds or those of any other person;
- a potential buyer (and its agents and advisers) in connection with any proposed purchase, merger or acquisition of any part of our business, provided that we inform the buyer it must use the insureds' personal information only for the purposes disclosed in our Privacy Policy; or
- any other person with the insureds' consent to the disclosure.

The personal information may be transferred to, and processed in, countries other than the country in which the insureds are resident. These countries may have data protection laws that are different to the laws of the country of the insureds. We transfer data within the Tokio Marine group of companies by virtue of our Intra Group Data Transfer Agreement, which includes the EU Standard Contractual Clauses.

We use appropriate technical and organisational measures to protect the personal information that we collect and process. The measures we use are designed to provide a level of security appropriate to the risk of processing the personal information.

The insureds are entitled to know what data is held on them and to make what is referred to as a Data Subject Access Request ('DSAR'). They are also entitled to request that their data be corrected in order that we hold accurate records. In certain circumstances, they have other data protection rights such as that of requesting deletion, objecting to processing, restricting processing and in some cases requesting portability. Further information on the insureds' rights is included in our Privacy Policy.

The insureds can opt-out of marketing communications we send them at any time. They can exercise this right by clicking on the "unsubscribe" or "opt-out" link in the marketing e-mails we send them. Similarly, if we have collected and processed their personal information with their consent, then they can withdraw their consent at any time. Withdrawing their consent will not affect the lawfulness of any processing we conducted prior to their withdrawal, nor will it affect processing of their personal information conducted in reliance on lawful processing grounds other than consent. The insureds have the right to complain to a data protection authority about our collection and use of their personal information.

Signature:

Please duly sign and send this Proposal Form to: Tokio Marine HCC, Torre Diagonal Mar, Josep Pla 2, Planta 10, 08019 Barcelona, Spain. Or via email to: cyber@tmhcc.com

Name:
Position:
Date:

Signature:

Declaration

I/we confirm that the information given in this Proposal Form, whether in my/our own hand or not, is correct.

I/we declare that I/we have made a fair presentation of the risk by disclosing all material matters and circumstances which would influence a prudent insurer's assessment of the risk which we know or ought to know including my/our senior management or anybody responsible for arranging my/our insurance, having conducted a reasonable search of the information available to me/us (including information held by third parties) in order to reveal those facts and circumstances. Failing that, I/we have given the Insurer sufficient information to put a prudent insurer on notice that it needs to make further enquiries in order to reveal material matters or circumstances, whether or not those matters and circumstances were the subject of a specific question in this Proposal Form. If there are any material matters or circumstances not specifically covered by a question in this Proposal Form, I/we have listed these on a separate sheet of paper which is signed and dated and attached.

It is understood that the signing of this Proposal Form does not bind the Proposer(s) to complete or the Insurer to accept the insurance applied for.

I/we the Proposer(s) accept these conditions as the proposed Insured or agent of the proposed Insured and that any subsequent Contract of Insurance may become null and void if any of the foregoing conditions are breached.

I/we the Proposer(s) accept these conditions as the Proposed Insured or agent of the Proposed Insured.

I/we the Proposer(s) also agree that in the event any information contained in any completed Proposal Form and/or supplied to support this Proposal Form or other application for the insurance applied for changes or becomes incorrect such as to constitute a material alteration to the risk prior to the inception date of the insurance, we will advise the Insurer in writing immediately on becoming aware of such changes. In such circumstances, the Insurer will be entitled to re-assess the proposal for insurance, including but not limited to withdrawing any prior agreement to provide cover.

The person signing this Proposal Form is duly authorised to do so on behalf of the Proposer(s).