Cyber Insurance Application form

Organisations are increasingly reliant on technology to drive core business objectives, while cyber risks have grown exponentially in recent years. In this rapidly changing environment, cyber insurance is more important than ever, and our end-to-end risk solution helps you stay ahead of the curve by helping you manage your cyber risk.

Cyber-attacks and incidents

Cyber-attacks and incidents are the most volatile risks facing businesses today. Ransomware for example can result in downtime of customer facing or backend systems and can hugely impact operations while intensifying regulation means tougher notification requirements.

Coverage

With the AIG Cyber Insurance, we can help mitigate such exposures and protect you if the worst does occur. As example:

Event Management After a cyber-attack, organisations will require a range of expert services to get their business back on track.

Business Interruption (loss of income) cover such losses from security breaches or system failures, even when occurring at Outsourced Service Providers.

Data breaches privicy liability and includes defence costs and insurable fines in relation to any regulator of Data Protection legislation.

Cyber Extortion extensive range of specialist services to combat the use of ransomware for cyber extortion.

Emergency First Response

The first 48 hours are vital when responding to a cyber incident and AIG's First Response service delivers best-in-class legal and IT forensics within 1 hour of ringing our hotline. This service can be used whenever clients have (or even suspect) a cyber incident, with no policy retention, without prejudicing policy coverage and without eroding the policy limits.

Why AIG's Cyber Insurance?

Complementary Loss Control Services
Our Cyber Insurance solution includes a host of complimentary and discounted tools and services to provide knowledge, awareness training (>30 languages), security tools and consultative solutions for clients purchasing Cyber Insurance.

Best in class coverages
Modular coverages sections with the below differentiators:

- All coverage sections offered as a standard.
- Business interruption identification periods up to 365 days.
- System failure and Voluntary Shutdown of IT systems.
- Cost conducting investigations to validate a threat, containment, and negotiations to end extortions through to ransom payments.
- No exclusions for widespread events or late patched systems / applications

Underwriting and claims excellence
Over 20 years of deep worldwide experience of our cyber underwriting and claims teams..

Cyber Insurance

AIG Cyber insurance application form - organizations up to 500M revenue

This application form is meant for organizations with a total group revenue up to 500M. Applicants with a revenue >500M or activities in high-risk industries should fill out the appropriate application form which can be downloaded here www.aiginsurance.nl. The following industries are considered high risk: Airlines, Aviation, Financial Institutions, Hospitals and healthcare facilities/practices, Law Firms, Managed Service Providers (MSP) and Managed Security Service Providers (MSSP), Payment Processors, and Public Entities (including Municipalities) and Schools (including primary, secondary schools and universities).

"***Applicant***" refers individually and collectively to each person or entity requested to be covered under this insurance. The completed information provided in this Application will be used to determine the extent and possibilities for an insurance offer.

"***Insurer***" shall mean the insurance company affiliate of American International Group, Inc. that issues the policy to the Applicant based on this Application. AIG Europe S.A. is an insurance undertaking incorporated under the laws of Luxembourg with R.C.S. Luxembourg number B218806. AIG Europe S.A. has its head office at 35D Avenue J.F. Kennedy, L-1855 Luxembourg. http://www.aig.lu/.

General Information

Full name of Applicant:	
Applicant is:	◯ Parent ◯ Subsidiary
Applicant's Web Page(s):	
Applicant's number of employees:	
Applicant's estimated annual revenue:	

Geograhical revenue

Select the region(s) the Applicant operates in. Total % of revenue must be equal to 100% (select all that apply).

Australia and New-Zealand	%	Russia	%
Canada	%	Mexico, Central America, and Caribbean	%
United States	%	South America	%
East-Asia and the Pacific	%	United Kingdom	%
Europe (ex UK)	%	South Africa	%
Central and Southern Asia	%		
Middle-East and North Africa	%	**Total**	**%**

Cyber Insurance

Please enter the following information for the ***Applicant's*** Chief Information Security Officer (CISO), or equivalent employee, that is responsible for maintaining the ***Applicant's*** cybersecurity posture.

Name:
Title:
E-mail:

*The **Insurer** may, but is under no obligation to, (1) use externally observable data about the **Applicant's** computer network, and (2) contact the **Applicant's** Chief Information Security Officer (or other person designated above) in connection with a condition or circumstance that the **Insurer** reasonably believes may result in a future event for which coverage may be afforded under the policy being applied for. The **Insurer** may continue to observe and report, as described above, during the term of any policy containing coverage issued to the **Applicant**.*

Dataprocessing

Please fill in the amount of data of each category that ***Applicant*** collects, processes, stores, or are transferred within the ***Applicant's*** environment, including records collected, processed, or stored by others for the ***Applicant***.

Unique Personally Identifiable Information (PII) records (including employees PII records):		
Unique Protected Health Information (PHI) records:	or	◯ Not applicable
Number of unique Payment Card Information (PCI):	or	◯ Not applicable
Number of Unique biometric identifiers:	or	◯ Not applicable

Industry

Select in which industries ***Applicant*** operates in. Total % of revenue must be equal to 100%.

Accountants	%	Payment processing	%
Agriculture, Forestry, Mining, Fishing, and Hunting	%	Real Estate	%
Attorneys	%	Retail Trade	%
Collection Agents	%	Information, Software, and Technology (excl. payment-processing)	%
Construction	%	Telemarketing	%
Credit Bureaus	%	Employment agency, recruitment services and payrolling	%
Dining / Restaurants	%	Third party administrators	%
Education (related)	%	Transportation & Warehousing	%
Financial Institutions	%	Travel Agencies	%
Financial services (Other than financial institutions)	%	Wholesale Trade	%
Professional, Scientific, and Technical Consultants	%	Utilities	%
Gaming, including casinos	%	Waste Management, Remediation Services, Administration and Support	%
Government entities	%	Not Listed (please specify)	%
Healthcare and Social Assistance	%		
Hotels / Lodging	%		
Manufacturing	%		
Media related entities	%	**Total**	**%**

AIG

Cyber Insurance

Exposure Section

a. Does the Applicant utilize Microsoft Active Directory Domain Services ("ADDS"), whether "on prem", hosted, or in a hybrid configuration? To the avoidance of doubt: with ADDS we explicitly DO NOT refer to Azure Active Directory ("Azure AD") or Microsoft Entra ID. Yes ◯ No ◯

b. Does the Company utilize Microsoft Exchange, including in a "hybrid deployment"? Yes ◯ No ◯

c. Does the Company utilize any unsupported software (software the vendor is no longer providing security fixes for)? Yes ◯ No ◯

Controls Section

Please indicate the controls within ***Applicant's*** environment. For this matter 'environment' means both the internal as well as the outsourced part of ***Applicant's*** environment. Should a response not fit 100% the Applicant's situation, please select "No" and provide additional information on the nuances where necessary either in the designated comment boxes at every page or in a separate document.

1. Backups and disaster recovery capabilities

a. A process for creating regular backups exists (even if it is undocumented and/or ad hoc). Yes ◯ No ◯

b. Backup strategy includes regular offline backups (either onsite or offsite). Yes ◯ No ◯

c. Backups are isolated and separate from the production domain (i.e. cloud backups with MFA protection) or they are are immutable. Yes ◯ No ◯

d. A document incident response plan is in place. Yes ◯ No ◯

2. Remote authentication (please select one answer)

Remote access to the corporate resources generally only requires a valid username and password (single factor authentication). ◯

MFA is required and enforced for all remote access for employees to the corporate network, and all exceptions to the policy are documented. ◯

MFA is required and enforced for all remote access (employee, vendors and 3rd party SaaS), and all exceptions to the policy are documented. ◯

Remote access to the corporate resources is not provided at all. ◯

3. Password policies

a. There's a password manager provided to all employees Yes ◯ No ◯

b. There's a policy in force against password reuse (uses unique passwords for apps in the environment) Yes ◯ No ◯

c. Service accounts (accounts used by machines - not people - for running applications and other processes) have password lengths of at least 25 characters. Yes ◯ No ◯

Comment box previous sections

4. Monitoring & response

a. There is a "Security Information and Event Monitoring" (SIEM) tool in place. Yes ◯ No ◯

b. The environment is monitored for traffic for anomalous and potentially suspicious data transfers. Yes ◯ No ◯

c. There is a "Security Operations Center" or SOC in place to monitor security incidents, internally and/or serviced by an MSSP (Managed Security Services Provider). Yes, 24/7 ◯ Yes, but not 24/7 ◯ No ◯

d. There is an incident response plan documented with specific focus on Cyber incident management. Yes ◯ No ◯

5. Phishing Defense: people

a. Security awareness training is in place, including phishing awareness training, to employees at least annually. Yes ◯ No ◯

b. Simulated phishing attacks are used to test employees' cybersecurity awareness at least annually. Yes ◯ No ◯

c. There is a documented process to report suspicious e-mails to an (internal) security team to investigate. Yes ◯ No ◯

6. Phishing Defense: technical

a. E-mails are 'tagged' or otherwise marked as outside the organization. Yes ◯ No ◯

b. An e-mail filtering solution is in place which blocks known malicious attachments and suspicious file types, including executables. Yes ◯ No ◯

c. A web-filtering solution is in place. Yes ◯ No ◯

d. The web-filtering solution has capabilities that are effective on all organization assets, even if the asset is not on the organization's network (e.g., assets are configured to utilize cloud-based web filters or require a VPN connection to browse the internet). Yes ◯ No ◯

7. Endpoint security tools

a. The endpoint security solution includes antivirus with heuristic capabilities and/or tools with behavioural-detection and exploit-mitigation capabilities. Yes ◯ No ◯

b. There is an endpoint threat detection and response (ETDR or EDR) tool in place which does the following: indicators; identifies patterns which match known threats; automatically responds by removing or containing threats; alerts security personnel of incidents; provides forensic and analysis capabilities to allow analysts to perform threat hunting activities. Yes ◯ No ◯

Comment box previous sections

8. Scope of Endpoint security tools

a. The endpoint security solution mentioned in the previous question is deployed on all workstations and laptops. Yes ◯ No ◯

b. The endpoint security solution mentioned in the previous question are deployed is deployed on all servers. Yes ◯ No ◯

c. For the endpoint security solution mentioned in the previous question, automatic updates are enabled. Yes ◯ No ◯

d. The endpoint security solution mentioned in the previous question is configured to block (vs. just notify of) suspected malicious processes/files. Yes ◯ No ◯

9. Patching

a. What is the capability to deploy the highest priority patches outside the regular periodic patching processes? (for example in the case of an in-the-wild exploitation of software for which an out-of-band patch is available)? 0-3 days ◯ 3-7 days ◯ >7 days ◯

b. Are regular vulnerability scans of externally exposed environments being performed? Yes ◯ No ◯

10. Segmentation and protection

a. There are network and/or host firewall rules implemented that prevent the use of external facing RDP (Remote Desktop Protocol) to log into workstations. Yes ◯ No ◯

b. There is an inventory of all service accounts (accounts used by machines - not people - for running applications and other processes. Yes ◯ No ◯ We don't have any service accounts ◯

c. Network firewalls have been implemented on all of ***Applicant's*** locations. Yes ◯ No ◯

11. Data Protection

Data is encrypted on end-user devices to safeguard data against lost devices. Example implementations include Windows Bitlocker, Apple FileVault, and Linux dm-crypt. Yes ◯ No ◯

Comment box previous sections

Outsourced Service Providers Section

Please provide the name of the third-party provider(s) you use for each of the following categories. If the ***Applicant*** does not use a third-party provider and capabilities/services or the category is not applicable to the ***Applicant's*** business operations, check N/A box for such category. If there are other third-party providers that are impactful to the ***Applicant's*** business that are not listed, use the Write-In Other(s) section.

Hosting Services

- ◯ N/A.
- ◯ Accenture
- ◯ Akamai
- ◯ Amazon AWS
- ◯ Atos
- ◯ AT&T
- ◯ CloudFlare
- ◯ Dell
- ◯ Equinix
- ◯ Fujitsu
- ◯ F5 Networks
- ◯ Gandi SAS
- ◯ Google
- ◯ HCL Technologies
- ◯ Hewlett Packard
- ◯ IBM
- ◯ Microsoft
- ◯ Newfold Digital
- ◯ OVH SAS
- ◯ Rackspace
- ◯ Siemens
- ◯ Telefonica
- ◯ United Internet AG
- ◯ Verizon
- ◯ Wipro
- ◯ Write-In Other(s):

E-Mail & Related Services

- ◯ N/A
- ◯ Amazon AWS SES
- ◯ AppRiver, LLC
- ◯ Barracuda Networks
- ◯ CyrenCorporation
- ◯ GoDaddy
- ◯ Google
- ◯ Intuit Mailchimp
- ◯ MailChannels
- ◯ McAfee, Inc
- ◯ Microsoft
- ◯ Mimecast
- ◯ Proofpoint
- ◯ Rackspace
- ◯ SendGrid, Inc
- ◯ Symantec
- ◯ United Internet AG
- ◯ Write-In Other(s):

Relationship/ CRM Software

- ◯ N/A
- ◯ Aptean
- ◯ Astute
- ◯ Atos
- ◯ Deltek
- ◯ eGain
- ◯ Gainsight
- ◯ Google
- ◯ Infor
- ◯ Medallia Inc
- ◯ Microsoft
- ◯ Oracle
- ◯ Sage Group
- ◯ Salesforce.com
- ◯ SAP
- ◯ Veeva Systems
- ◯ Zoho Corporation
- ◯ Write-In Other(s):

HR Management

- ◯ N/A
- ◯ ADP
- ◯ Avature Recruiting
- ◯ Ceridian
- ◯ Cornerstone
- ◯ Fujitsu
- ◯ HCL Technologies
- ◯ iCIMS
- ◯ IBM
- ◯ Jobvite
- ◯ Kronos
- ◯ NICE Systems
- ◯ Oracle
- ◯ PeopleAdmin
- ◯ PeopleFluent
- ◯ SAP
- ◯ WorkDay
- ◯ Xactly Corporation
- ◯ Write-In Other(s):

E-Commerce & Payment Services

- ◯ N/A
- ◯ Adyen B.V
- ◯ Amazon AWS
- ◯ Apple
- ◯ Atos
- ◯ BlueSnap
- ◯ CCBill
- ◯ EverCommerce
- ◯ Fidelity National Information Services
- ◯ Fujitsu
- ◯ Ingenico
- ◯ Klarna AB
- ◯ NCR Corporation
- ◯ PayPal
- ◯ Recurly
- ◯ Square
- ◯ Stripe
- ◯ VeriFone Systems
- ◯ Write-In Other(s):

Industrial Control Providers

- ◯ N/A
- ◯ ABB
- ◯ Bosch
- ◯ Emerson
- ◯ GE
- ◯ Honeywell
- ◯ Metso
- ◯ Mitsubishi Electric
- ◯ Rockwell Automation
- ◯ Rolls Royce
- ◯ Schneider
- ◯ Siemens
- ◯ Toshiba
- ◯ Yokogawa
- ◯ Write-In Other(s):

Security Service Providers

- ◯ N/A
- ◯ Accenture
- ◯ Akamai
- ◯ Atos
- ◯ Carbon Black
- ◯ Cisco
- ◯ CloudFlare
- ◯ Comodo Group
- ◯ CrowdStrike
- ◯ Dell
- ◯ DigiCert
- ◯ Fujitsu
- ◯ GMO GlobalSign
- ◯ HCL Technologies
- ◯ Hewlett Packard
- ◯ IBM
- ◯ Let's Encrypt
- ◯ McAfee
- ◯ Microsoft
- ◯ Okta
- ◯ Palo Alto
- ◯ Sentinel One
- ◯ Siemens
- ◯ Symantec
- ◯ Tenable Network
- ◯ TrustWave Holdings
- ◯ Unisys
- ◯ Verizon
- ◯ Wipro
- ◯ Write-In Other(s):

Cyber Insurance

Prior Claims, Circumstances & Warranties Section

1. Did the ***Applicant*** experience any of the below incidents in the past 5 years that had an impact on business operations?

a. Ransomware — Yes ◯ No ◯

b. Significant data / privacy breaches — Yes ◯ No ◯

c. Other security incidents with a significant impact — Yes ◯ No ◯

*** If yes on any of the above questions, please provide per incident the below information:**

- Incident summary and a description of the root cause of the incident.
- The improvements made to the environment to prevent a future attack.
- If there's a forensic report available, please send us a copy.
- An (estimation) of the total loss incurred, including but not limited to fees of forensic IT, legal, PR, cost of recovery business interruption and liability etc.)

2. Does the ***Applicant*** have any establishment, subsidiary, participation or joint venture and/or does the ***Applicant*** conduct business (with partners) in countries subject to sanctions imposed by the United Nations, the United States of America, the European Union or the country the handling AIG office resides in? Yes ◯ No ◯

3. In the past 5 years has:

a. insurance been refused for the ***Applicant*** or other related party in this application? Yes ◯ No ◯

b. the ***Applicant*** experienced a decline or cancelation of an insurance contract by another insurance company? Yes ◯ No ◯

c. an insurance contract been proposed to the prospective policyholder under restrictive or special conditions? Yes ◯ No ◯

d. a claim for cover of the candidate policyholder been completely or partially rejected? Yes ◯ No ◯

e. damage been claimed by an ***insurer*** from the candidate policyholder in connection with false statements? Yes ◯ No ◯

4. Has the ***Applicant*** or any other interested party in this insurance been in contact with the police or judicial authorities in the past eight years, as suspect or in execution of an (punitive) measure imposed in connection with: illegally obtained or to be obtained advantage, such as theft, embezzlement, deception, fraud, forgery or attempted attempt; unlawful prejudice against others, such as destruction or damage, mistreatment, extortion and diversion or any crime directed against personal freedom or against life or attempt (s) to this end; violation of the Weapons and Ammunition Act, the Opium Act or the Economic Offenses Act? Yes ◯ No ◯

If so, please indicate which offense was involved, whether it has been brought to trial, what the result was and whether any (punitive) measures have already been implemented. If it has not been a case, indicate whether there has been a settlement with the Public Prosecution Service, and if so, under what conditions the settlement was reached.

5. If you have answered Yes to any of the previous questions full details of each matter must be advised before quotation can be considered. We must remind you that it is imperative to answer these questions correctly. Please comment below. If there is insufficient space for answering the questions, please add additional information on your own paper.

No-claim declaration

Does the ***Applicant*** have knowledge of a situation or circumstance such as but not limited to any occurrences, Claims or Losses related to a failure of security of the ***Applicant's*** computer systems or has anyone filed suit or made a Claim against the ***Applicant*** with regard to invasion or interference with rights of privacy, wrongful disclosure of Confidential Information which might result in a Claim against the ***Applicant*** with regard to issues related to the ***Insurance Sought***?

- ◯ Yes
- ◯ No
- ◯ Not applicable (***Insurance Sought*** is renewal of the coverage with the Insurer)

It is agreed that with respect to the above, if any such occurrences, Claims, Losses or knowledge exists, then any Loss or Claim arising from such occurrences, Claims, Losses or knowledge shall be excluded from the proposed coverage.

Signature Section

Duly authorized representative, by and on behalf of the Applicant.

Name:	Signature:
Function:	
E-mail address:	
Location:	
Date:	

ADDITIONAL DOCUMENTS AND INFORMATION INCORPORATED BY REFERENCE

ALL WRITTEN STATEMENTS, MATERIALS OR DOCUMENTS FURNISHED TO THE ***INSURER*** IN CONJUNCTION WITH THIS APPLICATION, REGARDLESS OF WHETHER SUCH DOCUMENTS ARE ATTACHED TO THE POLICY, ARE HEREBY INCORPORATED BY REFERENCE INTO THIS APPLICATION AND MADE A PART HEREOF, INCLUDING WITHOUT LIMITATION ANY SUPPLEMENTAL APPLICATIONS OR QUESTIONNAIRES.

ANY SECURITY ASSESSMENT, ALL REPRESENTATIONS MADE WITH RESPECT TO ANY SECURITY ASSESSMENT, AND ALL INFORMATION CONTAINED IN OR PROVIDED BY ***APPLICANT*** WITH RESPECT TO ANY SECURITY ASSESSMENT, REGARDLESS OF WHETHER SUCH DOCUMENTS, INFORMATION OR REPRESENTATIONS ARE ATTACHED TO THE POLICY, ARE HEREBY INCORPORATED BY REFERENCE INTO THIS APPLICATION AND MADE A PART HEREOF.

LEGAL NOTICE AND SIGNATURES

BEFORE YOU SIGN THIS APPLICATION, READ THESE NOTICES CAREFULLY AND DISCUSS WITH YOUR BROKER IF YOU HAVE ANY QUESTIONS.

FOR THE PURPOSES OF THIS APPLICATION, THE UNDERSIGNED DULY AUTHORIZED REPRESENTATIVE OF ALL PERSONS AND ENTITIES PROPOSED FOR THIS INSURANCE DECLARES THAT, TO THE BEST OF HIS/HER KNOWLEDGE AND BELIEF, AFTER REASONABLE INQUIRY, THE STATEMENTS IN THIS APPLICATION, AND IN ANY ATTACHMENTS, ARE TRUE AND COMPLETE. THE UNDERSIGNED DULY AUTHORIZED REPRESENTATIVE AGREES THAT IF THE STATEMENTS AND INFORMATION SUPPLIED IN THIS APPLICATION OR INCORPORATED BY REFERENCE CHANGES BETWEEN THE DATE OF THIS APPLICATION AND THE EFFECTIVE DATE OF THE INSURANCE, HE/SHE (UNDERSIGNED) WILL, IN ORDER FOR THE INFORMATION TO BE ACCURATE ON THE EFFECTIVE DATE OF THE INSURANCE, IMMEDIATELY NOTIFY THE ***INSURER*** OF SUCH CHANGES, AND THE ***INSURER*** MAY WITHDRAW OR MODIFY ANY OUTSTANDING QUOTATIONS AND/OR AUTHORIZATIONS OR AGREEMENTS TO BIND THE INSURANCE.

SIGNING OF THIS APPLICATION DOES NOT BIND THE ***APPLICANT*** OR THE ***INSURER*** TO COMPLETE THE INSURANCE, BUT IT IS AGREED THAT THIS APPLICATION AND ANY INFORMATION INCORPORATED BY REFERENCE HERETO, SHALL BE THE BASIS OF THE CONTRACT SHOULD A POLICY BE ISSUED, AND IS INCORPORATED INTO AND IS PART OF THE POLICY.

SHOULD ***INSURER*** ISSUE A POLICY, ***APPLICANT*** AGREES THAT SUCH POLICY IS ISSUED IN RELIANCE UPON THE TRUTH OF THE STATEMENTS AND REPRESENTATIONS IN THIS APPLICATION OR INCORPORATED BY REFERENCE HEREIN. ANY MISREPRESENTATION, OMISSION, CONCEALMENT OR INCORRECT STATEMENT OF A MATERIAL FACT, IN THIS APPLICATION, INCORPORATED BY REFERENCE OR OTHERWISE, SHALL BE GROUNDS FOR THE RESCISSION OF ANY POLICY ISSUED.

NOTICE TO ***APPLICANTS***: ANY PERSON WHO KNOWINGLY AND WITH INTENT TO DEFRAUD ANY INSURANCE COMPANY OR OTHER PERSON FILES AN APPLICATION FOR INSURANCE OR STATEMENT OF CLAIM CONTAINING ANY MATERIALLY FALSE INFORMATION OR, CONCEALS, FOR THE PURPOSE OF MISLEADING, INFORMATION CONCERNING ANY FACT MATERIAL THERETO, COMMITS A FRAUDULENT ACT, WHICH IS A CRIME AND MAY SUBJECT SUCH PERSON TO CRIMINAL AND CIVIL PENALTIES.

APPLICANT AGREES THAT THE INFORMATION IN THIS APPLICATION MAY BE USED TO PROVIDE OR IMPROVE RISK MANAGEMENT PRODUCTS, SERVICES OR PROGRAM OFFERINGS.

If you have any questions that you have already known to the ***insurer***, you should answer as fully as possible. If you have not (fully) complied with your obligation to communicate, this may result in a restriction or even lapse of the entitlement to benefits. If you have intentionally acted to mislead the ***insurer*** or the ***insurer*** would not have concluded the insurance contract with knowledge ofthe true state of affairs, the ***insurer*** also has the right to terminate the insurance contract.

If permitted by law the following principles also apply to the obligation to provide information for this insurance application:

- An unanswered or open question is deemed to have been answered in the negative;
- The 'final question' must be answered in full. The 'final question' is deemed to have been answered incompletely if facts and circumstances have been omitted or misrepresented by the ***applicant***, for example on the basis of the other questions asked on the application form and / or the nature of the insurance applied for in relation to what has not been stated or was misrepresented, it must have been reasonably understood that these could be important for the assessment of the risk offered for insurance.