Cyber Security Insurance
Proposal Form

This proposal must be completed and signed by a Principal, Partner or Director of the Proposer. The person completing and signing the form should be authorised by the Proposer to do so and should make all necessary enquiries of his fellow Partners, Directors and Employees to enable all the questions to be answered. All questions must be answered to enable a quotation to be given. Completing and signing this proposal does not bind the Proposers or Insurers to enter a contract of insurance.

Contact Details

Contact Name:

Name:

Correspondence Address:

Company:

Address:

City/Town:

County:

Post Code

Country:

E-mail:

Phone:

Company Information

1. Please provide the following details (including trading names) of the Proposer/s:

Company Name	
Number of Employees	
Date of Establishment	
Website Address	

2. If you require cover for any associated, previous or subsidiary company please provide company names, including, if appropriate, details of any joint venture:

	Name	Location (city/town)	Nature of Business
1.			
2.			
3.			
4.			
5.			

3. Please provide a description of your business activities:

4. Please advise:

	Past year ending	Whole year current estimate	Estimate coming year
Total turnover including fee income	£	£	£

5. Estimated percentage split of your turnover including fee income for:

	Past year ending	Whole year current estimate	Estimate coming year
Work carried out for UK clients	%	%	%
Work carried out for US/Canadian clients not subject to US/Canadian Law	%	%	%
Work carried out for US/Canadian clients subject to US/Canadian Law	%	%	%
Work carried out for clients anywhere else in the world	%	%	%
Operating profit	%	%	%

Network and Data Structure

6. Please can you provide a financial value for your IT network (including but not limited to hardware, software, cabling and firmware):

£

7. Please can you estimate the total number of Personally Identifiable Information records, including employees and customers that your company holds:

Personally Identifiable Information is defined as: 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.

8. Do you see this changing substantially in the next 12 months?

◯ Yes ◯ No

If yes, please provide details below:

9. Please highlight which bands of Personally Identifiable Information records you hold:

	Yes	No
Low sensitivity	◯	◯
Moderate sensitivity	◯	◯
High sensitivity	◯	◯

Sensitivity Level Definitions

- Low sensitivity: Name, email address.
- Moderate sensitivity: home address, protected health information, telephone numbers, Insurance Policy number, date of birth, National Insurance number, Driver's Licence number, Passport number.
- High Sensitivity: banking or saving account number, debit card number, credit card number.

10. **Please estimate what proportion of the total number of Personally Identifiable Information records which you hold that include a highly sensitive element:**

%

11. **Do you seek explicit consent from all third parties before selling or sharing any Personally Identifiable Information:**

Yes No

Comments:

12. **Please provide brief details of the functions of your internal IT network:**

13. **Do you outsource any part of your IT network including but not limited to data storage, data hosting and/ or data processing of Personally Identifiable Information records?**

Yes No

If yes go to Q13a, b & c. If no go to Q14

13a. Please provide the name of the third-party company:

13b. Do you ensure that the countries in which these third-parties hold your Personally Identifiable Information records have strict government legislation and regulation on data protection?

Yes No

If no please provide details below:

13c. Do you have a written contract in place with these third parties that will indemnify you for IT system or data security breaches arising from their services?

Yes No

If no please provide details below:

14. When recruiting new employees do you undertake thorough background checks before employment is offered? Such as CRB (Criminal Records Bureau), Identity, Qualifications

Yes No

If no please provide details below:

Effects of an Incident

15. How fast are you likely to incur a loss of profit as a result of an IT network compromise and a total system downtime?

Level 1: 48 hours+

Level 2: 24-48 hours

Level 3: 12-24 hours

Level 4: 1-12 hours

Level 5: Immediately

16. In the event of your IT network being subjected to a non-scheduled closure and total downtime, please estimate your maximum daily loss of income/revenue:

£

17. **Do you have a disaster recovery plan which protects you against any sudden or unexpected failure of your IT network and security breach/data compromise?**

Yes No

If yes go to Q17a, If no go to Q17b

17a. If yes

Is the backup system managed by a third party?	Yes	no
How regularly is it tested?		
When was it last tested?		
How long does it take to switch to this backup system?		

17b. If no, please advise how you would deal with such an event in a time critical manner..

Risk Management Information

18. **Do you have a board level employee responsible for cyber security?**

Yes No

If yes, please provide details:

19. **Do you adhere to and comply with the following where relevant: Data Protection Act 1998; Privacy and Electronic Communications Regulations; Payment Card Industry (PCI) Data Security Standards; ISO27001 ?**

Yes No

Comments:

20. **Do you ensure that all Personally Identifiable Information records are backed up and held at a secondary location?**

Yes No

Comments:

21. **Do you have firewalls protecting all external IT network gateways?**

Yes No

Comments:

22. **Do you use encryption tools to ensure the integrity and confidentiality of all Personally Identifiable Information records including those on removable media?**

Yes No

Comments:

23. **Do you have anti-virus software and anti-spyware operational?**

Yes No

Comments:

24. **Do you control unauthorised access to your Computer systems by correctly configuring your wireless network?**

Yes No

Comments:

25. **Do you change all passwords on your Computer system at least every 60 days and cancel any usernames, password or other security protection once an employee's employment is terminated or after you knew or had reasonable grounds to suspect that usernames or passwords had become available to any unauthorised person?**

Yes No

Comments:

26. **Do you have an operational system for logging and monitoring user activity on your Computer System?**

Yes No

Comments:

27. **Do you have a remote wipe function installed and enabled on all portable devices where such functionality is available?**

Yes No

Comments:

28. **Do you have a vulnerability assessment program that monitors for IT network security and data security breaches?**

Yes No

Comments:

29. **Do you ensure timely updates of anti-virus and anti-spyware signatures and critical security patches?**

Yes No

Comments:

30. **Do you have an internet and email usage policy written into all employment contracts which is clearly communicated to all employees?**

Yes No

Comments:

31. **Do you implement a data protection policy for the handling of data including Personally Identifiable Information records which is clearly communicated to all employees?**

Yes No

Comments:

32. **Are all Personally Identifiable Information records, including those contained in a physical form (paper, disks, CDs, hard drives), disposed of or recycled by a confidential secure means which is recognised throughout the organisation?**

Yes No

Comments:

33. **Do you have a privacy policy on your website?**

Yes No

Comments:

34. **Do you have a specific policy for managing all "opt-in"/"opt-out" marketing requests including the use/ storage of cookies on a browser's system/device?**

Yes No

Comments:

35. **Do you have a procedure for responding to allegations that content created, displayed or published is libellous, infringing intellectual property rights, or in violation of a third-party's privacy rights?**

Yes No

Comments:

36. **Do you have a "take-down" policy which allows you to remove any third party content applied to any of your message boards, chat rooms or forums on your websites (including websites you may host for third-parties)?**

Yes No

Comments:

37. **Do you obtain written warranties and indemnities from third parties for content they have created for you (including advertising agents)?**

Yes No

Comments:

38. **Has your business ever been declined for a Cyber and Data Security insurance policy, or had an existing policy cancelled?**

Yes No

Comments:

39. **Have you ever experienced an event that did or may have given rise to a claim or circumstance under a cyber and data security policy, including but not limited to hacking incident, virus or malicious code attack, cyber extortion attempt, breach of secure data, wrongful disclosure of personal data or interference with rights of privacy?**

Yes No

Comments:

40. Do you provide all staff with continued online security training?

Yes No

Comments:

Please read this paragraph carefully before signing the declaration:

It is essential that every Proposer or Insured when seeking a quotation to take out or renew any insurance discloses to the prospective Insurers all material facts and information (including all material circumstance that is or should be known to anyone working within the business) that might influence the judgement of an underwriter in deciding whether to accept the risk and on what terms. The obligation to provide this information continues up to and beyond the time when there is a completed contract of insurance. Failure to do so entitles the Insurers, should they so wish, to void the contract of insurance from inception and so enables them to repudiate liability thereunder. If you have any doubt as to what constitutes a material fact or circumstance please ask for advice. Further information on the Insurance Act is available here or on request.

DECLARATION

I/We declare that, after full enquiry, the contents of this proposal are true and that I/We have not misstated, omitted or suppressed any material fact or information. I/We agree that this proposal together with any other information supplied by me/us shall form the basis of any contract of insurance which may be effected. If there is/are any materials alteration to the facts and information which I/We have provided or any new material matter arising before the completion of the contract of insurance, I/We undertake to inform Insurers.

I/We hereby consent to any information I/We have provided being processed by you for the purposes of providing insurance and claims handling, which may necessitate sharing such information with third parties. BGi.uk may use this information for marketing (by post, telephone, e-mail or fax) subject to the conditions of the Data Protection Act. If you do not wish these details to be used for marketing please inform BGi.uk in writing. Under the Data Protection Act 1998 you have the right to access or amend the information we hold about you. If you would like to exercise either of these rights please contact BGi.uk.

Declaration:

☐ I acknowledge that the information here-in is true and correct and forms the basis on which the insurance is provided.

Date form completed:

dd/mm/yyyy

Please return the completed form by:

Email: cyber@BGi.uk.com
Uploading: BGi.uk.com/upload
Post: BGi.uk, Portwell House, Market Place, Faringdon, Oxfordshire SN7 7HU.