Cyber large corporate
Insurance application form

US

The purpose of this application form is for us to find out more about you. You must provide us with all information which may be material to the cover you wish to purchase and which may influence our decision whether to insure you, what cover we offer you or the premium we charge you.

How to complete this form

The individual who completes this application form should be a senior member of staff at the company and should ensure that they have checked with other senior managers and colleagues responsible for arranging the insurance that the questions are answered accurately and as completely as possible. Once completed, please return this form to your insurance broker.

Section 1: Company Details

1.1 Please state the name and address of the principal company for whom this insurance is required. Cover is also provided for the subsidiaries of the principal company, but only if you include the data from all of these subsidiaries in your answers to all of the questions in this form.

Company name:

Primary address (Address, State, ZIP, Country):

1.2 Date business was established (MM/DD/YYYY):

1.3 Number of employees: Website:

1.4 Date of company financial year end (MM/DD/YYYY):

1.5 Please state your gross revenue in respect of the following years:

	Last complete FY	Estimate for current FY	Estimate for next FY
Domestic revenue:	$	$	$
Other territory revenue:	$	$	$
Total gross revenue:	$	$	$
Profit (Loss):	$	$	$

Primary contact details

To allow us to provide information about downloading our incident response app and receiving risk management alerts and updates, please provide contact details for the most relevant person within your organisation for receiving such updates:

Contact Name: Position:

Email Address: Telephone Number:

Section 2: Activities

2.1 Please describe below the products and services supplied by your business:

2.2 Please provide an approximate breakdown of how your revenue is generated from your products and services within the following categories:

Sales direct to customer: % Sales made on a contract or subscription basis: %

Sales made online: %

2.3 Please state what percentage of these customers are domiciled in the US: %

Section 3: Data Storage

3.1 Please indicate the approximate volume of data relating to private individuals that you store on your systems or with third party processors:

Data type	Number of unique records
Name	
Email	
Passport number	
Medical record	
Social security number	
Financial information	
Payment card number	
Biometric information	

3.2 Please describe your approach towards the encryption of sensitive and confidential data that you are responsible for:

3.3 Do you encrypt all sensitive data when it is stored on portable devices? ☐ Yes ☐ No

3.4 Do you ensure all outsourcing contracts provide you with full indemnification in the event of a breach of confidential data, including sensitive personal data? ☐ Yes ☐ No

Section 4: Network Dependancy

4.1 Please identify your top three most critical business applications, including the name of the application, the business process that it supports and the financial impact of this application being unavailable for 24 hours (including additional resource costs and potential loss of profits):

Application name	Description	Vendor	Host	Outage Impact (24hr)

Section 5: IT Infrastructure & Resourcing

5.1 Please provide a high-level overview of your IT infrastructure, including details on whether it is predominantly on-premise or cloud based:

5.2 Please state the approximate number of:

a) servers on your network:

b) desktops and laptops on your network:

5.3 Please provide details of major IT system implementations or migrations that have taken place in the last year and details of any that are planned in the next 12 months:

5.4 Who is responsible for IT security within your organisation?

Role	Name	Email

5.5 Please state the following in respect of the person detailed in the question above:

a) do they have board level responsibility: ☐ Yes ☐ No

b) how many years have they been in the role?

5.6 Please state:

a) your annual IT budget: $

b) the approximate percentage of your IT budget that is spent on IT security: %

5.7 How many full-time employees do you have in your IT department?

5.8 How many full-time employees are dedicated to a role in IT security?

5.9 Please provide details on whether you have a Security Operations Centre ("SOC") that is responsible for event monitoring and detection, vulnerability management and incident response. Please include details on the hours of operation and whether this is an internal function or outsourced to a third party:

Section 6: Cyber Security Controls

6.1 Please state whether you have a fully documented information security policy: ☐ Yes ☐ No

6.2 Please describe your patch management process and how you ensure that all critical patches are applied in a timely fashion:

6.3 What is your target time to deploy critical patches as per your patching policy:

6.4 Do you use any software that is no longer supported by the manufacturer (e.g. Windows XP)? ☐ Yes ☐ No

If "yes", please provide details on the number of devices running such software and describe any compensating controls you have in place to prevent these sytems being exploited:

6.5 Please confirm whether multi-factor authentication is required for all remote access to your network: ☐ Yes ☐ No

6.6 Please confirm whether multi-factor authentication is required for all remote access to email: ☐ Yes ☐ No

6.7 Please confirm whether multi-factor authentication is required to access all cloud-based resources where you store confidential and sensitive data: ☐ Yes ☐ No

6.8 Please describe how you protect privileged user accounts. Please include details on any use of internal multi-factor authentication and/or privileged access management tools:

6.9 Do your non-IT users have administrative rights on their laptops/ desktops? ☐ Yes ☐ No

6.10 Please state which endpoint protection product(s) you use:

6.11 Please state which endpoint detection and response (EDR) product(s) you use:

6.12 What percentage of workstations and servers have EDR applied: %

6.13 Is your EDR tool monitored internally or is it an externally managed solution:

6.14 Please provide details on any controls in place designed to limit lateral movement (e.g. network segmentation, RDP restrictions etc.):

6.15 Please provide details of any internationally recognised standards for information governance (e.g. ISO 27001) that you comply with:

6.16 How frequently do you test employees with simulated phising attacks:

6.17 Please tick all the boxes below that relate to controls that you currently have implemented within your IT infrastructure (including where provided by a third party):

☐ Employee Phishing Training	☐ Application Whitelisting	☐ Asset Inventory	☐ SPF
☐ Database Encryption	☐ Data Loss Prevention	☐ DDoS Mitigation	☐ DMARC
☐ DNS Filtering	☐ Privileged Access Management	☐ Incident Response Plan	☐ DKIM
☐ Intrusion Detection System	☐ Email Filtering	☐ Next Generation Firewalls	☐ Security Info & Event Management
☐ Two-factor Authentication	☐ Custom Threat Intelligence	☐ Web Application Firewall	☐ Web Content Filtering

6.18 Please provide the name of the software or service provider that you use for each of the controls highlighted above:

Section 7: Assessments

7.1 How often do you conduct vulnerability scanning of your network perimeter?

7.2 How often do you conduct vulnerability scanning of your internal network?

7.3 What percentage of the enterprise is covered by scheduled scans? (%)

7.4 How often do you conduct penetration testing of your network architecture?

7.5 Please state whether you have implemented all high and critical security recommendations from your most recent security tests: ☐ Yes ☐ No

7.6 If you process cardholder data, are all your cardholder data environments certified as being PCI compliant? ☐ Yes ☐ No

7.7 If "yes", please state the version you are currently compliant with:

7.8 If PCI compliant, please provide details of the certification date and name of the QSA that conducted the certification:

7.9 Please provide details of any internal or third-party assessments that you have undertaken in the last 12 months to assess the efficacy of your security controls (e.g. red teaming, security maturity assessments, audits etc.)

Section 8: Backup and Recovery

8.1 Please state whether you have a fully documented and tested:

a) cyber incident response plan: ☐ Yes ☐ No

b) disaster recovery plan: ☐ Yes ☐ No

c) business continuity plan: ☐ Yes ☐ No

8.2 Have you conducted a ransomware tabletop exercise in the last 12 months: ☐ Yes ☐ No

8.3 Please state whether you have a disaster recovery facility for all your critical systems and data: ☐ Yes ☐ No

8.4 Please describe the high-level configuration of your disaster recovery systems:

8.5 Please provide the recovery time objective (RTO) and recovery point objective (RPO) for your main mission critical IT systems as per the current business continuity plan or disaster recovery plan:

8.6 Please describe your backup process for critical data. Please include details of the frequency of back-ups, number of backup copies taken, and backup media used:

8.7 Please state whether backups are disconnected from and inaccessible through your network: ☐ Yes ☐ No

8.8 How often do you test system restoration capabilities from infrastructure and user data backups:

8.9 Do you utilise multi-factor authentication to restrict access to your backups? ☐ Yes ☐ No

Section 9: Claims Experience

9.1 Please provide details of all major systems outages in the last 5 years where the outage has lasted for longer than 5 hours and the estimated financial impact was above $50,000:

9.2 Please state whether you:

a) have experienced a data breach involving more than 500 records in the last 5 years: ☐ Yes ☐ No

b) have ever been investigated by any national or state level data protection regulator or any industry regulator in relation to data security issues: ☐ Yes ☐ No

c) are aware of any claims, loss, damage or circumstances which may give rise to a claim against any of the companies to be insured or any of their partners or directors: ☐ Yes ☐ No

If you have answered "yes" to any of the above then please describe the incident, including the monetary amount of the potential claim or the monetary amount of any claim paid or reserved for payment by you or by an insurer. Please include all relevant dates, including a description of the status of any current claim which has been made but has not been settled or otherwise resolved.

Important Notice

By signing this form you agree that the information provided is both accurate and complete and that you have made all reasonable attempts to ensure this is the case by asking the appropriate people within your business. CFC Underwriting will use this information solely for the purposes of providing insurance services and may share your data with third parties in order to do this. We may also use anonymized elements of your data for the analysis of industry trends and to provide benchmarking data. For full details on our privacy policy please visit www.cfcunderwriting.com/privacy

Contact Name: Position:

Signature: Date (MM/DD/YYYY):