Cyber private enterprise

Insurance application form

Basic company details

Please complete the following details for the entire company or group (including all subsidiaries) that is applying for the insurance policy. Any defined terms will be bolded and highlighted in blue and can be found in the glossary at the end of this application form:

Company name: Primary industry sector:

Primary address (address, state, ZIP, country):

Description of business activities:

Website address:

Date established (MM/DD/YYYY): Number of employees:

Last 12 months gross revenue: $ Revenue from international sales (%):

Last 12 months gross profit: $

Please state which financial institution(s) you use for your commercial banking:

Primary contact details

Please provide contact details for the individual within your organization who is primarily responsible for IT security. These details will be used to provide information about downloading our incident response app and receiving risk management alerts and updates:

Contact name: Position:

Email address: Telephone number:

Previous cyber incidents

Please tick all the boxes below that relate to any cyber incident that you have experienced in the last three years (there is no need to highlight events that were successfully blocked by security measures):

☐ Cyber extortion ☐ Data loss ☐ Denial of service attack ☐ IP infringement

☐ Malware infection ☐ Privacy breach ☐ Ransomware ☐ Theft of funds

☐ Other (please specify)

If you ticked any of the boxes above, did the incident(s) have a direct financial impact upon your business of more than $10,000? ☐ Yes ☐ No

If 'yes', please provide more information below, including details of the financial impact and measures taken to prevent the incident from occuring again:

Revenue analysis

Please provide the following details for your top 5 clients:

Name of client:	Primary services:	Annual revenue derived from client:

Cyber private enterprise

Insurance application form

IT infrastructure and resourcing

Please confirm the name of your managed service provider (if applicable):

What is the approximate number of servers on your network?

What is the approximate number of desktops and laptops on your network?

What is your annual IT budget?

What approximate percentage of your IT budget is spent on IT security?

Is any part of your IT infrastructure outsourced to third party technology providers, including application service providers? ☐ Yes ☐ No

If you answered "yes" to the question above, please list your critical third party technology providers below (up to a maximum of 10), including a brief summary of the technology services they provide for you:

Data storage and management

Please provide the approximate number of unique individuals that you collect, store and/or process personally identifiable information from, whether on your own systems or with third parties:

Data type	Number of unique individuals
Sensitive data (e.g. medical records, passport details, social security numbers etc)	
Non-sensitive data (e.g. full names, addresses, email addresses etc)	

Please describe your approach towards protecting sensitive and confidential information (e.g. access controls, encryption, network segmentation etc):

Please provide details of how often you purge records that are no longer required:

Please provide details on how you store your back-ups of critical data (e.g. online back-ups stored on your organisation's live environment, offline back-ups stored on a removable storage device that is fully disconnected and inaccessible from the live environment, back-ups stored with an online cloud storage provider etc.):

Please provide details on the frequency of your back-ups, including the frequency of full system back-ups and the frequency of incremental/ differential back-ups of critical data:

Please provide details on how you secure your back-ups (e.g. back-ups are disconnected and inaccessible from the live environment, multi-factor authentication is required for access to cloud back-ups etc):

Please provide details on how you test your back-ups, including details on how frequently you test the full restoration and recovery of key server configurations and data from back-ups:

Please provide details on the number of back-up copies you take, including details on how you prevent separate back-up copies being impacted by the same event (if applicable):

Cyber private enterprise

Insurance application form

Endpoint security

Which endpoint protection product do you use on your network?
Please provide the name of the vendor and the product used

Do you use an endpoint detection and response (EDR) product on your network? ☐ Yes ☐ No

If "yes":

Which product do you use:

Please provide an overview of how your EDR product is monitored and managed (e.g. internal IT team or outsourced to a third party):

Is the EDR product deployed on all endpoints on your network? ☐ Yes ☐ No

If "no":

What percentage of endpoints do not have EDR deployed and why is it not deployed on these endpoints:

Perimeter security

Do you have next-generation firewalls deployed at all network ingress/egress points? ☐ Yes ☐ No

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

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

Please provide details of the third party providers you use to conduct penetration testing (if applicable)

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

If you use an alternative method for securing remote access to your network, such as certificate based authentication for devices, please provide details here:

Please confirm whether multi-factor authentication is required to access *all cloud resources holding sensitive or confidential information* ☐ Yes ☐ No

Email security

Please confirm that multi-factor authentication is enabled for remote access to all company email accounts: ☐ Yes ☐ No

Do you simulate phishing attacks to test employees at least annually? ☐ Yes ☐ No

Do you use email filtering software to scan all inbound and outbound email messages in order to filter out spam and malicious content? ☐ Yes ☐ No

If you answered "yes" to the previous question, please state the name of the vendor and product used for email filtering:

If you are an Office 365 user, please provide your Microsoft Secure Score
(administrators can find the score using the following link https://security.microsoft.com/securescore):

Cyber private enterprise

Insurance application form

Network security

Please provide details on how you protect privileged user accounts (e.g. using privileged access management solutions, restricting privileged user accounts to specific devices, enhanced monitoring of accounts for anomalous usage, multifactor authentication enabled for remote access etc):

Do non-IT users have local administrator rights on their laptops/desktops? ☐ Yes ☐ No

Do you use a network monitoring solution to alert your organisation to suspicious activity or malicious behaviour on your network? ☐ Yes ☐ No

If you answered "yes" to the previous question, please state the name of the vendor and product used for network monitoring:

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:

Do you have any end of life or end of support software? ☐ Yes ☐ No

If "yes", please provide details on what the end of life or end of support software is, how it is used, whether it is segregated from the rest of the network and if so, how it is segregated:

Please describe your patch management process and how you ensure that all critical patches are applied in a timely fashion, including a timeframe of how quickly you would implement patches for zero day vulnerabilities after they have been released by the vendor:

Please provide details of any major changes that you have planned for your IT infrastructure in the next 12 months (if any):

Additional controls

Please confirm that **before** any change is made to a third party's account details, you obtain authorization from the third party via an authentication method which is different to the original method used to request the change? ☐ Yes ☐ No

Please confirm that **before** you transfer funds to an account that you haven't paid into before, you obtain authorisation from the recipient of the funds via an authentication method which is different to the original method used to request the transfer? ☐ Yes ☐ No

Do you provide training on phishing/social engineering scams for all employees involved in transferring funds on behalf of your organisation on at least an annual basis? ☐ Yes ☐ No

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). If you're unsure of what any of these tools are, please refer to the explanations on the final page of this document.

☐ Application whitelisting	☐ Asset inventory	☐ Custom threat intelligence	☐ Database encryption
☐ Data loss prevention	☐ DDoS mitigation	☐ DMARC	☐ DNS filtering
☐ Employee awareness training	☐ Incident response plan	☐ Intrusion detection system	☐ Perimeter firewalls
☐ Security info & event management	☐ Virtual private network (VPN)	☐ Web application firewall	☐ Web content filtering

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

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):

Glossary of terms

Application whitelisting

A security solution that allows organisations to specify what software is allowed to run on their systems, in order to prevent any nonwhitelisted processes or applications from running.

Asset inventory

A list of all IT hardware and devices an entity owns, operates or manages. Such lists are typically used to assess the data being held and security measures in place on all devices.

Custom threat intelligence

The collection and analysis of data from open source intelligence (OSINT) and dark web sources to provide organisations with intelligence on cyber threats and cyber threat actors pertinent to them.

Database encryption

Where sensitive data is encrypted while it is stored in databases. If implemented correctly, this can stop malicious actors from being able to read sensitive data if they gain access to a database.

Data loss prevention

Software that can identify if sensitive data is being exfiltrated from a network or computer system.

DDoS mitigation

Hardware or cloud based solutions used to filter out malicious traffic associated with a DDoS attack, while allowing legitimate users to continue to access an entity's website or web-based services.

DMARC

An internet protocol used to combat email spoofing – a technique used by hackers in phishing campaigns.

DNS filtering

A specific technique to block access to known bad IP addresses by users on your network.

Email filtering

Software used to scan an organisation's inbound and outbound email messages and place them into different categories, with the aim of filtering out spam and other malicious content.

Employee awareness

Training programmes designed to increase employees' security awareness. For example, programmes can focus on how to identify potential phishing emails.

Endpoint detection and response (EDR)

A software tool that works by monitoring and collecting data from endpoints and recording the information in a central database where further analysis, detection, investigation, reporting and alerting take place.

Endpoint protection

Software installed on individual computers (endpoints) that uses behavioural and signature based analysis to identify and stop malware infections.

Incident response plan

Action plans for dealing with cyber incidents to help guide an organisation's decision-making process and return it to a normal operating state as quickly as possible.

Intrusion detection system

A security solution that monitors activity on computer systems or networks and generates alerts when signs of compromise by malicious actors are detected.

Managed service provider

A third party organisation that provides a range of IT services, including networking, infrastructure and IT security, as well as technical support and IT administration.

Mobile device encryption

Encryption involves scrambling data using cryptographic techniques so that it can only be read by someone with a special key. When encryption is enabled, a device's hard drive will be encrypted while the device is locked, with the user's passcode or password acting as the special key.

Multi-factor authentication

Where a user authenticates themselves through two different means when remotely logging into a computer system or web based service. Typically a password and a passcode generated by a physical token device or software are used as the two factors.

Network monitoring

A system, utilising software, hardware or a combination of the two, that constantly monitors an organisation's network for performance and security issues.

Next-generation firewalls

Software or hardware solutions that combines traditional firewall technology with additional functionality, such as encrypted traffic inspection, intrusion prevention systems and anti-virus.

Penetration tests

Authorized simulated attacks against an organisation to test its cyber security defences. May also be referred to as ethical hacking or red team exercises.

Perimeter firewalls

Hardware solutions used to control and monitor network traffic between two points according to predefined parameters.

Security info & event management (SIEM)

System used to aggregate, correlate and analyse network security information – including messages, logs and alerts – generated by different security solutions across a network.

Security Operations Centre (SOC)

A facility that houses an information security team responsible for monitoring and analysing an organisation's security posture on an ongoing basis. The SOC team's goal is to detect, analyse and respond to cybersecurity incidents using a combination of technology solutions and a strong set of processes. SOC's can be internal and run by the organisation themselves or outsourced to a third party.

Virtual private network (VPN)

A VPN is an encrypted connection over the internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. Most commonly used to provide a secure remote connection to an organisation's network.

Vulnerability scans

Automated tests designed to probe computer systems or networks for the presence of known vulnerabilities that would allow malicious actors to gain access to a system.

Web application firewall

Protects web facing servers and the applications they run from intrusion or malicious use by inspecting and blocking harmful requests and malicious internet traffic.

Web content filtering

The filtering of certain web pages or web services that are deemed to pose a potential security threat to an organisation. For example, known malicious websites are typically blocked through some form of web content filtering.