Cyber Proactive Response

Insurance application form

US

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:

If known, please provide the approximate number of unique individuals whose personal identifiable information you collect, store and/or process:

Primary contact details

Please provide contact details for the individual within your organisation 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:

CFC Underwriting Limited is Authorized and Regulated by the Financial Conduct Authority

© 1999-2026 CFC Underwriting Ltd, All Rights Reserved

IT infrastructure and resourcing

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

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:

Cyber security controls

Please confirm whether multi-factor authentication is enabled and enforced 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:

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

Do you use a network monitoring solution to alert your organisation to suspicious activity or malicious behavior 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 confirm that multi-factor authentication is enabled and enforced 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:

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:

CFC Underwriting Limited is Authorized and Regulated by the Financial Conduct Authority

© 1999-2026 CFC Underwriting Ltd, All Rights Reserved

Please describe your data back-up policy in detail, including how the back-ups are stored (e.g. online, offline, cloud storage etc), how frequently your back-ups are taken, how you secure your back-ups, how you test your back-ups and how regularly you test them, and how many back-up copies you take:

Additional controls

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	☐ Endpoint detection & response	☐ Incident response plan	☐ Intrusion detection system
☐ Next-generation firewalls	☐ Penetration testing	☐ Perimeter firewalls	☐ Security operations centre (SOC)
☐ Virtual private network (VPN)	☐ Vulnerability scanning	☐ 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.cfc.com***

Contact name: Position:

Signature: Date (MM/DD/YYYY):

CFC Underwriting Limited is Authorized and Regulated by the Financial Conduct Authority

© 1999-2026 CFC Underwriting Ltd, All Rights Reserved

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 behavioral 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.

CFC Underwriting Limited is Authorized and Regulated by the Financial Conduct Authority

© 1999-2026 CFC Underwriting Ltd, All Rights Reserved

ALABAMA FRAUD WARNING: Any person who knowingly presents a false or fraudulent claim for payment of a loss or benefit or who knowingly presents false information in an application for insurance is guilty of a crime and may be subject to restitution, fines or confinement in prison, or any combination thereof.

ARKANSAS FRAUD WARNING: Any person who knowingly presents a false or fraudulent claim for payment for a loss or benefit or knowingly presents false information in an application for insurance is guilty of a crime and may be subject to fines and confinement in prison.

CALIFORNIA FRAUD WARNING: For your protection California law requires the following to appear on this form. Any person who knowingly presents false or fraudulent information to obtain or amend insurance coverage or to make a claim for the payment of a loss is guilty of a crime and may be subject to fines and confinement in state prison.

COLORADO FRAUD WARNING: It is unlawful to knowingly provide false, incomplete, or misleading facts or information to an insurance company for the purpose of defrauding or attempting to defraud the company. Penalties may include imprisonment, fines, denial of insurance, and civil damages. Any insurance company or agent of an insurance company who knowingly provides false, incomplete, or misleading facts or information to a policyholder or claimant for the purpose of defrauding or attempting to defraud the policyholder or claimant with regard to a settlement or award payable from insurance proceeds shall be reported to the Colorado division of insurance within the department of regulatory agencies.

DISTRICT OF COLUMBIA FRAUD WARNING: It is a crime to provide false or misleading information to an insurer for the purpose of defrauding the insurer or any other person. Penalties include imprisonment and/or fines. In addition, an insurer may deny insurance benefits if false information materially related to a claim was provided by the applicant.

FLORIDA FRAUD WARNING: Any person who knowingly and with intent to injure, defraud, or deceive any insurer files a statement of claim or an application containing any false, incomplete, or misleading information is guilty of a felony of the third degree.

KANSAS FRAUD WARNING: Any person who, knowingly and with intent to defraud, presents, causes to be presented or prepares with knowledge or belief that it will be presented to or by an insurer, purported insurer, broker or any agent thereof, any written, electronic, electronic impulse, facsimile, magnetic, oral, or telephonic communication or statement as part of, or in support of, an application for the issuance of, or the rating of an insurance policy for personal or commercial insurance, or a claim for payment or other benefit pursuant to an insurance policy for commercial or personal insurance which such person knows to contain materially false information concerning any fact material thereto; or conceals, for the purpose of misleading, information concerning any fact material thereto commits a fraudulent insurance act.

KENTUCKY FRAUD WARNING: Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance containing any materially false information or conceals, for the purpose of misleading, information concerning any fact material thereto commits a fraudulent insurance act, which is a crime.

LOUISIANA FRAUD WARNING: Any person who knowingly presents a false or fraudulent claim for payment of a loss or benefit or knowingly presents false information in an application for insurance is guilty of a crime and may be subject to fines and confinement in prison.

MAINE FRAUD WARNING: It is a crime to knowingly provide false, incomplete or misleading information to an insurance company for the purpose of defrauding the company. Penalties may include imprisonment, fines or denial of insurance benefits.

MARYLAND FRAUD WARNING: Any person who knowingly or willfully presents a false or fraudulent claim for payment for a loss or benefit or who knowingly or willfully presents false information in an application for insurance is guilty of a crime and may be subject to fines and confinement in prison.

NEVADA FRAUD WARNING: Any person who includes any materially false or materially misleading information on an application for an insurance policy may be guilty of a crime and subject to penalties that include imprisonment, fines and denial of insurance benefits.

NEW JERSEY FRAUD WARNING: Any person who includes any false or misleading information on an application for an insurance policy is subject to criminal and civil penalties.

NEW MEXICO FRAUD WARNING: Any person who knowingly presents a false or fraudulent claim for payment of a loss or benefit or knowingly presents false information in an application for insurance is guilty of a crime and may be subject to civil fines and criminal penalties.

NEW YORK FRAUD WARNING: 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 insurance act, which is a crime, and shall also be subject to a civil penalty not to exceed five thousand dollars and the stated value of the claim for each such violation.

OHIO FRAUD WARNING: Any person who, with the intent to defraud or knowing that he is facilitating a fraud against an insurer, submits an application or files a claim containing a false or deceptive statement is guilty of insurance fraud.

OKLAHOMA FRAUD WARNING: Any person who knowingly, and with intent to injure, defraud or deceive any insurer, makes any claim for the proceeds of an insurance policy containing any false, incomplete or misleading information is guilty of a felony.

OREGON FRAUD WARNING: Any person who, with an intent to knowingly defraud or knowingly facilitate a fraud against an insurer, submits an application or files a claim containing a false or deceptive statement or a material fact, may be guilty of insurance fraud.

PENNSYLVANIA FRAUD WARNING: 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 insurance act, which is a crime and subjects such person to criminal and civil penalties.

PUERTO RICO FRAUD WARNING: Any person who knowingly and with the intention of defrauding presents false information in an insurance application, or presents, helps, or causes the presentation of a fraudulent claim for the payment of a loss or any other benefit, or presents more than one claim for the same damage or loss, shall incur a felony and, upon conviction, shall be sanctioned for each violation by a fine of not less than $5,000 and not more than $10,000, or a fixed term of imprisonment for 3 years, or both penalties. Should aggravating circumstances be present, the penalty thus established may be increased to a maximum of 5 years, if extenuating circumstances are present, it may be reduced to a minimum of 2 years.

RHODE ISLAND FRAUD WARNING: Any person who knowingly presents a false or fraudulent claim for payment of a loss or benefit or knowingly presents false information in an application for insurance is guilty of a crime and may be subject to fines and confinement in prison.

TENNESSEE FRAUD WARNING: It is a crime to knowingly provide false, incomplete, or misleading information to an insurance company for the purpose of defrauding the company. Penalties include imprisonment, fines, and denial of insurance benefits.

VERMONT FRAUD WARNING: Any person who knowingly presents a false statement in an application for insurance may be guilty of a criminal offense and subject to penalties under state law.

VIRGINIA FRAUD WARNING: It is a crime to knowingly provide false, incomplete, or misleading information to an insurance company for the purpose of defrauding the company. Penalties include imprisonment, fines, and denial of insurance benefits.

WASHINGTON FRAUD WARNING: It is a crime to knowingly provide false, incomplete, or misleading information to an insurance company for the purpose of defrauding the company. Penalties include imprisonment, fines, and denial of insurance benefits.

WEST VIRGINIA FRAUD WARNING: Any person who knowingly presents a false or fraudulent claim for payment of a loss or benefit or knowingly presents false information in an application for insurance is guilty of a crime and may be subject to fines and confinement in prison.