

# Application



## Cyber insurance

Please complete the following details for the entire company or group (including all subsidiaries) that is applying for the insurance policy and who share network interconnectivity.

Any defined terms are bolded and highlighted in orange and can be found in the Cybersecurity controls glossary at the end of this application form.

### Basic company details

1. Company name (legal entity and operating name if applicable): \_\_\_\_\_  
\_\_\_\_\_  
Primary industry sector: \_\_\_\_\_
2. Primary address: \_\_\_\_\_  
Province: \_\_\_\_\_ Postal code: \_\_\_\_\_ Country: \_\_\_\_\_
3. Description of business activities: \_\_\_\_\_
4. Website address: \_\_\_\_\_
5. Date established (dd/mm/yyyy): \_\_\_\_\_
6. Number of employees: \_\_\_\_\_
7. Last 12 months gross revenue: \$ \_\_\_\_\_ Revenue from U.S. sales: \_\_\_\_\_ %  
Last 12 months gross profit: \$ \_\_\_\_\_
8. 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.

9. Contact name: \_\_\_\_\_ Position: \_\_\_\_\_  
Email address: \_\_\_\_\_ Telephone number: \_\_\_\_\_

### Previous cyber incidents

10. 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):  
 Cyberextortion     Data loss     Denial of service attack     IP address infringement  
 Malware infection     Privacy breach     Ransomware     Theft of funds  
 Other (please specify): \_\_\_\_\_
11. If you ticked any of the boxes above, did the incident(s) have a direct financial impact 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 occurring again:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

## Revenue analysis

12. Please provide the following details for your top five clients:

Client name	Primary services	Annual revenue derived from client
		\$
		\$
		\$
		\$
		\$

## IT infrastructure and resourcing

13. Please confirm the name of your **managed service provider** (if applicable): \_\_\_\_\_

14. What is the approximate number of servers on your network? \_\_\_\_\_

15. What is the approximate number of desktops and laptops on your network? \_\_\_\_\_

16. What is your annual IT budget? \$\_\_\_\_\_

17. What approximate percentage of your IT budget is spent on IT security? \_\_\_\_\_%

18. Is any part of your IT infrastructure outsourced to third party technology providers, including application service providers? YES  NO

If yes, 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

19. 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.):	

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

---



---

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

---



---

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

---



---

23. Please provide details on the frequency of your backups, including the frequency of full system backups and the frequency of incremental/differential backups of critical data:

---

---

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

---

---

25. Please provide details on how you test your backups, including details on how frequently you test the full restoration and recovery of key server configurations and data from backups:

---

---

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

---

---

## Endpoint security

27. Which **endpoint protection** product do you use on your network? \_\_\_\_\_

Please provide the name of the vendor and the product used:

---

---

28. Do you use an **endpoint detection and response (EDR)** product on your network? YES  NO

If yes, which product do you use: \_\_\_\_\_

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

---

---

30. 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

31. Do you have **next-generation firewalls** deployed at all network ingress/egress points? YES  NO

32. How often do you conduct **vulnerability scanning** of your network perimeter? \_\_\_\_\_

33. How often do you conduct **penetration testing** of your network architecture? \_\_\_\_\_

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

---

---

35. Please confirm whether **multi-factor authentication** is required for **all remote access to your network**:

YES  NO

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

---

---

37. Please confirm whether **multi-factor authentication** is required to access **all cloud resources holding sensitive or confidential information**: YES  NO

## Email security

38. Please confirm that **multi-factor authentication** is enabled for remote access to **all company email accounts**: YES  NO

39. Do you simulate phishing attacks to test employees at least annually? YES  NO

40. 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 yes, please state the name of the vendor and product used for email filtering:

---

41. 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>):

---

## Network security

42. 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.):

---

---

43. Do non-IT users have local administrator rights on their laptops/desktops? YES  NO

44. Do you use a **network monitoring** solution to alert your organization to suspicious activity or malicious behaviour on your network? YES  NO

If yes, please state the name of the vendor and product used for network monitoring:

---

45. 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:

---

---

46. 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:

---

---

47. 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:

---

---

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

---



---

**Additional controls**

49. 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

50. Please confirm that, **before** you transfer funds to an account that you have not paid into before, you obtain authorization from the recipient of the funds via an authentication method which is different to the original method used to request the transfer: YES  NO

51. Do you provide training on phishing/social engineering scams for all employees involved in transferring funds on behalf of your organization on at least an annual basis? YES  NO

52. 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 are unsure of what any of these tools are, please refer to the explanations on the final page of this document.

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

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

---



---

**Limits and deductibles**

54. Please indicate the limits and deductibles you would like to obtain quotes for:

(a) Cyber and privacy

Limit	Deductible
<input type="checkbox"/> \$250,000	<input type="checkbox"/> \$2,500
<input type="checkbox"/> \$500,000	<input type="checkbox"/> \$5,000
<input type="checkbox"/> \$1,000,000	<input type="checkbox"/> \$10,000
<input type="checkbox"/> \$2,000,000	<input type="checkbox"/> \$15,000
<input type="checkbox"/> \$3,000,000	<input type="checkbox"/> \$20,000
Other (please specify):	Other (please specify):

(b) Cyber crime

Limit	Deductible
<input type="checkbox"/> \$50,000	<input type="checkbox"/> \$2,500
<input type="checkbox"/> \$75,000	<input type="checkbox"/> \$5,000
<input type="checkbox"/> \$100,000	<input type="checkbox"/> \$10,000
<input type="checkbox"/> \$150,000	<input type="checkbox"/> \$15,000
<input type="checkbox"/> \$250,000	<input type="checkbox"/> \$20,000
Other (please specify):	Other (please specify):

## Data protection

By accepting this insurance you consent to CFC Underwriting using the information they may hold about you for the purpose of providing insurance and handling claims, if any, and to process sensitive personal data about you where this is necessary (for example, health information or criminal convictions). This may mean we have to give some details to third parties involved in providing insurance cover. These may include insurance carriers, third party claims adjusters, fraud detection and prevention services, reinsurance companies and insurance regulatory authorities. CFC Underwriting may also use anonymized elements of your data for the analysis of industry trends and to provide benchmarking data. For full details on CFC Underwriting Privacy Policy, please visit [www.cfcunderwriting.com/privacy](http://www.cfcunderwriting.com/privacy).

Where such sensitive personal information relates to anyone other than you, you must obtain the explicit consent of the person to whom the information relates both to the disclosure of such information to CFC Underwriting and its use by them as set out above. The information provided will be treated in confidence and in compliance with relevant Data Protection legislation. You have the right to apply for a copy of your information (for which CFC Underwriting may charge a small fee) and to have any inaccuracies corrected.

## Important – Cyber insurance policy statement of fact

By accepting this insurance you confirm that the facts contained in the application form are true. These statements, and all information you or anyone on your behalf provided before CFC Underwriting agrees to insure you, are incorporated into and form the basis of your policy. If anything in these statements is not correct, CFC Underwriting will be entitled to treat this insurance as if it had never existed. You should keep this Statement of Fact and a copy of the completed application form for your records.

This application must be signed by the applicant. Signing this form does not bind the company to complete the insurance. With reference to risks being applied for in the United States, please note that in certain states, any person who, knowingly and with intent to defraud any insurance company or other person, submits an application for insurance containing any false information or conceals the purpose of misleading information concerning any fact material thereto, commits a fraudulent insurance act, which is a crime.

The undersigned is an authorized principal, partner, director, risk manager or employee of the applicant and certifies that reasonable inquiry has been made to obtain the answers herein which are true, correct and complete to the best of his/her knowledge and belief. Such reasonable inquiry includes all necessary inquiries to fellow principals, partners, directors, risk managers or employees to enable you to answer the questions accurately.

---

Contact name (please print)

---

Position

---

Signature

---

Date (dd/mm/yyyy)

## Application whitelisting

A security solution that allows organisations to specify what software is allowed to run on their systems, in order to prevent any non-whitelisted 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 cyberthreats and cyberthreat 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

Training programs designed to increase employees' security awareness. For example, programs 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 cybersecurity 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 organization'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 organization 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 organization'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.