QBE

QBE QCyberProtect
Enterprise Any One Claim

Quick Quote Form

Last updated January 2026

Why do you need Cyber Liability Insurance?

Specialist advisers available 24/7 to help you deal with a cyber and/or privacy incident

Your IT systems are crucial an outage is detrimental to your service and reputation

Cost of a cyber event is often more than expected

Everyone is a target with the abundance of phishing emails and rogue links being sent to employees

As well as peace of mind you receive access to the QCyberPrepare platform, an out of band safe room, built to empower you to be connected and in control before, during and after an incident

QCyberPrepare

Confidence before, during and after a cyber incident

During a cyber incident, there may be uncertainty that an organisation's files, documents and communication channels are available or clear of threat actors. QCyberPrepare (powered by CYGNVS) enables an organisation to securely store key documents (plans, policies, key contacts etc.) and effectively communicate outside the corporate network.

QCyberPrepare can be an organisation's cyber saferoom, ensuring an efficient and coordinated approach when a cyber incident occurs.

QCyberPrepare, in partnership with CYGNVS, is built to empower organisations to be connected, confident, and in control before, during and after a cyber crisis.

Key benefits include:

- User friendly cyber response platform to help organisations proactively prepare for cyber incidents.
- Confidential and secure storage for critical documents and contact information, ensuring accessibility even if an organisational network becomes compromised during a cyber incident.
- An out-of-band solution with access controlled by your organisation.
- Invite and collaborate with your incident response team, including external advisors, to prepare for a cyber incident.
- 24/7 secure access to incident response documents and messaging capabilities so your business can launch incident response processes as soon as an incident occurs.
- Secure messaging and video call capabilities.

Opportunity

QCyberPrepare is available to all QBE Primary Cyber insurance customers.

For more information

Please contact
QCyberServices@qbe.com

What does the QCyberProtect - Enterprise AOC Policy cover?*

Third Party Liability

- **Network Security & Privacy Cover including PCI DSS compliance** - Covers defence costs and damages from security breaches and privacy violations
- **Regulatory Defence & Penalties** - Protection against privacy regulation violations and associated regulatory proceedings
- **Digital Media Protection** - Cover for website, social media, and intranet content liability including defamation and copyright issues
- **Bodily Injury/Property Damage Cover** - cover for Bodily Injury or Property Damage arising from an Event.

Incident Response, Support & Recovery

- **Comprehensive Event Cover** - Includes forensics, data restoration, credit monitoring, and PR expenses, plus network betterment costs to upgrade affected systems beyond their pre-incident state
- **Cyber Extortion Protection** - Covers costs to address and investigate cyber extortion threats
- **Business Interruption** - Compensation for net income loss and additional expenses from network breaches, system failures, or necessary shutdowns, including cover for interruptions caused by dependent IT and non-IT service provider incidents
- **First Response Coverage** - Immediate access to expert panel (forensics, legal, PR) with no retention
- **Claims Preparation Support** - Cover for forensic accounting services.

Extended Protection

- **Hardware Replacement** - Covers devices rendered non-functional by cyber attacks
- **Reputational Damage** - Lost income cover from adverse publicity following privacy or security breaches
- **Cryptocurrency Protection** - Cover for increased utility costs from cryptojacking incidents
- **Reward Funds** - Cover for reward payments leading to cybercriminal convictions.

Cyber Crime

- **Social Engineering** - Cover for losses from fraudulent transfer instructions
- **Funds Transfer Fraud** - Protection against unauthorised financial transfers by financial institution
- **Invoice Manipulation** - Cover for losses from fraudulent invoice payment redirection
- **Telephone Fraud** - Cover for increased service charges from telephone fraud events.

*For the full policy summary, please see pages (6-9) of this document.

How much does it cost? *(excluding applicable tax)*

The below premium is subject to industry sector eligibility and the completion of Section 2 of this form to the satisfaction of QBE.

Industry	Please select from the following
Turnover	Please select from the following
Limit	Please select from the following
Retention	
Premium	

Coverage

Full limits any one claim for all Insured Sections.

The following Insured Sections, where applicable, are limited to:

- £50,000 Bodily Injury/Property Damage Coverage
- 10% Additional Increased Cost of Working
- Full limit for Dependent Business Interruption Coverage
- £50,000 Reward Fund Coverage
- Full policy limit or £250,000 Cryptojacking Coverage, whichever is lowest, Telephone Fraud
- Full policy limit or £250,000 Cyber Crime, including Social Engineering, Funds Transfer Fraud, Invoice Manipulation and Telephone Fraud
- Coverage, whichever is lowest
- £50,000 Claims Preparation Costs
- 10% Betterment Percentage.

Other cover specifications, where applicable:

- **72 Hours:** First Response Coverage Time Period
- **8 Hours:** Waiting Period for Business Interruption, Dependent Business Interruption and Consequential Reputational Loss Coverage
- **365 Days:** Period of Recovery for Business Interruption, Dependent Business Interruption and Consequential Reputational Loss Coverage.

Any One Claim (AOC) Coverage

Policyholders benefit from any one claim coverage, which applies the **full policy limit to each individual claim**. This means that if the policyholder experiences unrelated events during the same policy period, such as both a ransomware attack and a separate unrelated business email compromise in the same policy year, each incident is covered up to the full limit - no sharing, no compromise.

Why AOC Coverage?

- **Full limit payout per incident** - No dilution across multiple unrelated claims
- **Up to £5million coverage limits** - flexible limit options, ranging from £100,000 to £5 million
- **Value for money** - policyholders pay a single premium regardless of how many claims are made
- **Protection throughout the lifespan of the policy** - policyholders can be confident they are protected throughout the whole policy period.

AOC coverage gives policyholders peace of mind and clarity so they can focus on what they do best - running their business.

This form is applicable only to proposers with total gross revenue of £100 million or less that are headquartered within the United Kingdom and have operations within the United Kingdom and Europe. If you have operations within Europe, please ask your broker to complete and send us a tax schedule. Signing or completing this form does not bind the proposer, or any individual or entity he or she represents, to complete this insurance.

To apply for a QCyberProtect - Enterprise AOC Policy please complete the Quick Quote Form below:

1 Your business		
Insured name		
Gross revenue – last completed financial year (GBP)		
Business type	Please select from the following	Please select from the following
Address		
Website		

2 Statement of fact	
Please confirm that you are NOT a	True ☐ False ☐
a) Health or social care provider b) An entity which has exposure to nuclear power c) Internet service provider or telecommunications service provider d) Government entity, public body, council, local authority, political party or lobbying group e) Payment processor or involved in cryptocurrency or financial technology company f) School, college or university g) Social networking, pornography, blogging/vlogging, dating website, mobile application, video game developer, or gambling company h) Franchisee, franchisor or subsidiary of a larger organisation i) Aviation and airport j) Energy company	
Please confirm if the statements below are true or false	
a) We do not collect, store or process more than 3,000,000 personal data records	True ☐ False ☐
b) Multi-Factor Authentication (MFA) is required for all forms of remote access to your systems, including but not limited to VPN, RDP, and cloud services.	True ☐ False ☐
c) Multi-Factor Authentication (MFA) is required for all web-email account access. *Please say 'True' if web-based email access is not permitted.*	True ☐ False ☐
d) Organisation-wide awareness campaigns for social engineering (such as phishing, vishing, and smishing) are conducted at least once a year.	True ☐ False ☐
e) One or more of the following email protocols are implemented: DMARC, DKIM, and SPF.	True ☐ False ☐
f) Two or more of the following email controls are implemented. - Tagging of external emails - Malware scanning for malicious links and attachments - Email quarantine service implemented - Email sandboxing solution implemented - Email Data Loss Prevention (DLP) solutions.	True ☐ False ☐
g) An anti-malware solution and/or an endpoint protection platform has been deployed on all company devices.	True ☐ False ☐
h) A policy for managing and installing critical patches for systems exposed to the internet has been established.	True ☐ False ☐
i) Backups are segmented from the main network and secured with separate credentials accessible only to privileged users. If not segmented from the network, immutable backups are employed.	True ☐ False ☐
j) There is a formal, documented process for verifying the legitimacy of wire transfer requests, especially when there are changes to existing vendor information or for transactions above a certain threshold.	True ☐ False ☐
k) There is a multi step approval process in place for wire transfers, including segregation of duties and additional verification for transfer above a specified amount.	True ☐ False ☐
l) In the past 3 years, we have not had any cyber or data breach incidents or other incidents that would otherwise have been covered under this policy had it been in force at the time.	True ☐ False ☐

3 Other Information
If you replied 'False' to any of the above statements please advise why and what provisions you have in place to mitigate the risk

4 Conditions		
Wording to apply:	QCyberProtect - Enterprise AOC	
Retroactive date:	Full retroactive cover	
If a QBE Cyber renewal, please provide the policy number:		
Period cover to apply from: 12 months from	Date	/ /

5 Declaration			
I/We declare that this proposal has been completed after appropriate enquiry and that the statements and particulars in this proposal (including all attachments, if applicable) are true and that I/We have neither misrepresented or withheld any material facts. I/We undertake to inform underwriters of any material alteration to these facts whether occurring before or after the completion of the contract of insurance. Quote is valid for 30 days from date that the declaration is signed below.			
Title			
Print name			
Signature		Date	/ /
Email address			
Form checked by (office use only)			

Policy Summary of Key Terms & Conditions

Underwritten by a member of the qbe insurance group (qbe) (details are provided below)

This insurance is an annual contract unless stated otherwise and it may be renewed at the end of each policy year on the basis of the terms and conditions applicable upon renewal. For full details of the start date and end date of the policy, you should read the policy schedule.

This document provides only an indicative summary of the main benefits of your insurance policy. The policy's significant features and benefits are outlined below together. The summary then provides an overview of any important exclusions or limitations. For full details of all policy benefits and all terms, you should read the policy.

The policy is divided into a number of sections but not all the sections may be operative as part of your insurance. Please refer to your quotation or renewal documentation for confirmation of the sections of cover selected.

Maximum liability, limits of liability, territorial limit and jurisdictional limit

This insurance is subject to a maximum liability for each Incident. The maximum limit is the combined Limit of Liability for all Liability Coverages and/or all Reimbursement Coverages under this policy, as applicable. Individual Cyber Crime Coverages are subject to their own Limit of Liability. The Limit of Liability for Cyber Crime Coverage and Defence Costs are all part of, not in addition to, the maximum liability. The cover available under this policy is not subject to any territorial limits. However, certain sections of the policy are restricted according to the applicable law of this policy (England & Wales), as well as any relevant trade and sanctions laws. Please refer to your policy schedule for confirmation of the applicable limits, and territorial and jurisdictional limits.

Retention

With the exception of First Response Expenses, any claims made against the policy will be a subject to a retention. You are responsible for paying the retention amount. The retention amounts will vary according to the type of loss. The retention amounts will be stated in your Policy Schedule, as well as any quotation or renewal documentation. Please refer to your policy document for details of how the retention operates.

Event

In your policy, the word 'Event' is a defined term that we use to mean certain scenarios involving a breach of privacy or network security. These include your failure to prevent/protect against: unauthorised access, unauthorised use of or denial of access to a computer network; a computer network being used in a Denial of Service Attack against a third party or to transmit malicious code that harms a third party; disclosure or theft of confidential information by you or someone you are legally responsible for; theft of hardware containing data; or a breach of your legal duty to disclose any of these failures.

We also use 'Event' to refer to situations where you fail to implement or follow privacy policies concerning confidential information, or where a breach of privacy or network security listed above results in a breach of your legal duties relating to confidential information. Please refer to your policy document for details of 'Event' and other defined terms.

Insuring Agreements

A. Liability Coverages

1. **Network Security and Privacy Liability Coverage (including Payment Card Industry Data Security Standard known as PCI-DSS)**
   Significant features and benefits
   This policy covers defence costs and damages as result of a claim first made against you during the policy period for an alleged Event.

2. **Privacy Regulatory Proceeding Coverage**
   Significant features and benefits
   This policy covers defence costs and regulatory damages as a result of a privacy regulatory proceeding first made against you during the policy period, which alleges an Event resulted in the violation of a privacy regulation.

3. **Media Liability Coverage**
   Significant features and benefits
   This policy covers defence costs and damages as a result of a claim first made against you during the policy period for any defamation, infringement of copyright, invasion of privacy or misappropriation of ideas arising from publishing content on your website, intranet or social media.

4. **Bodily Injury/Property Damage Coverage**
   Significant features and benefits
   This policy covers defence costs and damages as a result of a claim first made against you during the policy period for any Bodily Injury/Property Damage arising from an Event where you have a general liability insurance policy in force during the policy period.

B. Reimbursement Coverages

1. **Event Expense Coverage**
   Significant features and benefits
   This policy covers reasonable and necessary legal, forensics, data restoration, credit and ID monitoring, public relations and other expenses, which result from an Event first discovered during the policy period.

2. **Network Extortion Coverage**
   Significant features and benefits
   This policy reimburses reasonable and necessary expenses incurred as a result of an extortion threat first made during the policy period, including costs to terminate the extortion threat, and to investigate its cause.

3. **Business Interruption Coverage**
   Significant features and benefits
   This policy covers business interruption loss that is incurred during the period of recovery and which results from a business interruption (including where caused by an IT supplier) first occurring during the policy period.

4. **Dependent Business Interruption Coverage**
   Significant features and benefits
   This policy covers business interruption loss incurred during the period of recovery, which results from measurable harm to your business caused by a dependant business interruption (i.e. the unauthorised access to, use of or denial of access to the computer network of a business you contract with) first occurring during the policy period.

5. **Bricking Coverage**
   Significant features and benefits
   This policy covers hardware expenses incurred resulting from a breach of network security that renders a computer device or connected device non-functional for its intended purpose first discovered by you during the policy period.

6. **Consequential Reputational Loss Coverage**
   Significant features and benefits
   This policy covers loss of net income incurred during the period of recovery, which results from adverse publicity concerning a failure to prevent or protect against a breach of privacy or network security that is first discovered during the policy period.

7. **Reward Fund Coverage**
   Significant features and benefits
   This policy covers reward payments for information that leads to the arrest and prosecution of an individual who committed or attempted to commit any illegal act that caused any loss covered by this policy.

8. **Cryptojacking Coverage**
   Significant features and benefits
   This policy covers increased utility service charges or fees resulting from a breach of network security, which is first discovered during the policy period, and committed by a third party or rogue employee for the purpose of mining cryptocurrency .

9. **Cyber Crime Coverage**

   (1) Social Engineering Coverage
   Significant features and benefits
   This policy covers Social Engineering losses you incur after transfering money or securities to an account outside your control on the fraudulent instructions of someone impersonating one of your authorised employees, or an outsourced vendor, supplier or customer. However, this cover only applies to Social Engineering Events discovered during the policy period, and where you have followed suitable and established authentication procedures to validate the request prior to making the transfer.

   (2) Fund Transfer Coverage
   Significant features and benefits
   This policy covers Funds Transfer Losses you incur after a financial institution transfers money or securities on the fraudulent and unauthorised instructions of a third party impersonating you, where you first discover the Fund Transfer Fraud Event during the policy period.

   (3) Invoice Manipulation Coverage
   Significant features and benefits
   This policy covers losses you incur where unauthorised access to a computer network leads to your clients, customers or vendors being sent fraudulent payment instructions. This deception results in funds they transfer to pay your invoice being sent to a third party. However, this cover only applies to Invoice Manipulation Events that are first discovered by you during the policy period.

   (4) Telephone Fraud Coverage
   Significant features and benefits
   This policy covers increased utility service charges or fees you incur resulting from unauthorised access to or use of your company's telephone system by a third party or rogue employee. However, this cover only applies to Telephone Fraud Events that are first discovered by you during the policy period.

10. **First Response Coverage**
    Significant features and benefits
    This policy covers First Response Expenses for services provided by our Panel Advisor(s) (computer forensics, notifications, legal expenses, credit and identification monitoring services, data recovery, crisis management, and public relations) in response to an Event.

    We pay the Panel Advisors directly for First Response expenses covered under this policy, so you don't have to worry about cash flow. This helps ensure you have immediate access to expert assistance during critical incident response periods. This cover is not subject to a retention.

    The cover applies to First Response expenses incurred within the policy Time Period (usually 72 hours from the time you contact our 24-hr Hotline), which result from a relevant Event that you discover during the policy period.

Exclusions

A. False advertising or misrepresentation in the content on your website, intranet or social media pages.

B. Breach of competition, restraint of trade, or anti-trust legislation or regulations.

C. Your assumption of the liability of others arising under a contract. However, this exclusion does not apply to certain hold harmless or indemnity agreements set out in Media Liability Coverage section of the policy.

D. Bodily injury or property damage. However, this exclusion does not apply in respect of claims for bodily injury or any property damage resulting from a bricking event or for any claim under the Bodily Injury/Property Damage Coverage.

E. Claims by or on behalf of any insured. However, this exclusion does not apply in respect to certain claims from you when you are acting in your capacity as a customer, or for any claim under the Network Security and Privacy Liability Coverage, or Privacy Regulatory Proceeding Coverage.

F. Criminal, intentional, fraudulent or knowingly wrongful act, error or omission, or any wilful violation of any statute, rule or law by you. However, this exclusion will only apply where it is established that such conduct occurred by a final and non-appealable adjudication adverse to you in an underlying proceeding. Further, this exclusion does not apply to certain breaches of privacy or network security, or extortion threats by a rogue employee.

G. Over-redemption; or, subject to the Media Liability Coverage terms and conditions, gambling, promotional games or other games of chance detailed in the policy.

H. Employment practices wrongful acts by you in your capacity as an employer. However, this exclusion does not apply to any claim under Network Security and Privacy Liability Coverage, or Privacy Regulatory Proceeding Coverage, where it is made by a current or former employee of yours.

I. Violation of the Employee Retirement Income Security Act of 1974, Pensions Act 2008 or any similar federal, state, local or foreign statutory law. However, this exclusion does not apply to certain breaches of privacy or network security detailed in the policy.

J. Fee disputes.

K. Electronic fund transfer or transaction, theft of money, securities or other valuable consideration or financial trading loss. However, a narrower exclusion concerning customer/client accounts applies for the Cyber Crime Coverages.

L. Government action, or order by any domestic or foreign law enforcement, administrative, regulatory or judicial body or other governmental authority. This exclusion does not apply to any claim event expressly covered under the Network Security and Privacy Liability Coverage, the Privacy Regulatory Proceeding Coverage, or a claim brought by such entity when acting in the capacity as a customer.

M. Invalidity/validity, infringement, violation or misappropriation of any trade secret, copyright, service mark, trade name, trademark or trade dress. This exclusion does not apply to the Media Liability Coverage or to intellectual property related matters occurring as the direct result of an Event.

N. Actions brought involving intellectual property licensing rights organisations. With the exception of the Media Liability Coverage, the policy also excludes disputes over licensing rights and royalties/licensing fees.

O. Personal liability incurred in the role of a director or officer.

P. Electrical or mechanical failure of infrastructure or natural perils.

Q. Liability to pay PCI DSS Assessments in circumstances where you are not compliant with the Payment Card Industry Standards for Data Security.

R. Use of non-licensed software or firmware. This exclusion only applies to Bricking Coverage.

S. The infringement of any patent.

T. Pollution, including nuclear, chemical, biological and radioactive contamination.

U. Circumstance, claim, wrongful act or other event known prior to the beginning of the policy period or notified under a previous policy.

V. Purchase, sale, offer or solicitation of an offer to purchase or sell securities. However, this exclusion does not apply to any a failure to prevent or protect against a breach of privacy or network security.

W. Bodily injury, damage, claim, loss, liability, expenses, costs or defence costs caused by terrorism.

X. Unlawful or unauthorised collection, acquisition, retention, processing or use of data. However, this exclusion does not apply to a claim resulting from the acts of a rogue employee.

Y. Breach of unsolicited communications legislation or regulations. However, this exclusion does not apply to such unsolicited communications occurring as the direct result of an Event.

Z. Loss, bodily injury, claim, defence costs, damage, liability, cost or expense of any kind resulting from: war; a cyber operation that is part of a war; or a cyber operation that causes a major detrimental impact on the essential services and/or security of a sovereign state.

Premium Payment

You are liable to pay the premium as set out in the policy. The premium payment date is listed in your policy schedule. For full details of your premium and when it should be paid, you should read your quote and policy documents.

Other Restrictions

This policy is subject to a number of terms and conditions that are set out in full in the policy. Certain endorsements that might apply to your policy may restrict cover. For full details, you should read your policy documents.

Claim Notification

You must notify us of claims and circumstances that may become a claim as soon as practicable but always within the time limitation(s) stated in the policy.

The law and language applicable to the policy

This Policy and all disputes and claims arising under or relating to it, or to its subject matter or drafting (including non-contractual disputes, claims or actions), shall be governed by and construed in accordance with the law of England and Wales.

Complaints Procedure

If you are unhappy with the service provided for any reason or have cause for complaint you should initially contact the person who arranged the policy for you.

You can complain about the policy by contacting your broker or by contacting us using the complaints details below.

QBE UK Limited or QBE Europe SA/NV (UK Branch)
CustomerRelations@uk.qbe.com

Customer Relations, QBE European Operations,
30 Fenchurch Street, London EC3M 3BD

+44 (0)20 7105 5988

QBE Lloyd's syndicates complaints escalation

Where the QBE insurer is or includes a Lloyd's syndicate, and you are dissatisfied with the response you have received from QBE, you may escalate the complaint by using the complaints details below.

QBE's Lloyd's syndicates
Complaints@lloyds.com

Lloyd's Complaints, Fidentia House, Walter Burke Way,
Chatham Maritime, Kent ME4 4RN

+44 (0)20 7327 5693

The UK Financial Ombudsman Service (UK FOS)

If you feel that your complaint has not been satisfactorily resolved, you may be eligible to contact the UK FOS to review the complaint.

Information about the eligibility criteria is available on the UK FOS website https://www.financial-ombudsman.org.uk/consumers/how-to-complain.

Details on how to contact the UK FOS are as follows:

Financial Ombudsman Service
+44 (0)800 023 4567

financial-ombudsman.org.uk/consumers/how-to-complain

Financial Services Compensation Scheme (FSCS)

You may be entitled to compensation from the FSCS if we are unable to meet our obligations under the policy. Further information is available from **www.fscs.org.uk**, or you can write to the Financial Services Compensation Scheme, PO Box 300, Mitcheldean, GL17 1DY.

QBE European Operations
30 Fenchurch Street
London EC3M 3BD
+44 (0) 20 7105 4000
QBEeurope.com

928804/2602