

Made possible



CyberCrime

QBE Europe

@QBE_eo

Small and medium-sized businesses are increasingly being targeted by cyber criminals.

That's why QBE CyberCrime has been specially designed to provide comprehensive insurance cover for SMEs.



In line with our practice of developing innovative e-trade products going that bit farther, QBE CyberCrime is **the first e-trade product of its type** on the Acturis platform.

The product can include **Social Engineering Fraud** cover, **Cyber Business Interruption** cover and full **Crime** cover for greater peace of mind.

A rapid forensic response...

When an incident happens, a rapid response is vital. We've partnered with a data breach specialist to provide 24-hour a day assistance, including:



- Professional assessment of the issue
- IT forensics experts to investigate and help resolve the issue, either working remotely or with a site visit
- Legal advice throughout the claim
- Experian credit monitoring service
- Specialist Public Relations (PR) advice to help minimise any impact on the company reputation

Main benefits

- Fast e-trade quotes for around 3600 trades and professions, 24 hours a day
- Social Engineering Fraud cover automatically included where risk management acceptable (theft of money, property or goods by using fraudulent methods such as fake emails and phone calls)
- Core cyber covers included as standard
 - Data security and multimedia
 - Data breach notification costs
 - Information and communication asset rectification costs
 - Public relations costs
 - Forensics costs
 - Credit monitoring costs
 - Cyber extortion
 - Regulatory defence costs, including cover for Payment Card Industry (PCI) fines and legal investigation costs
- Option to add Cyber Business Interruption cover
- Option to add full Crime cover
- Delivery of policy documents when you want them puts you in control
- Comprehensive wording

Why choose QBE?

Because we make it possible.

As specialist insurance providers for almost every kind of business, our people have the experience, detailed knowledge and positive attitude you need to achieve your goals.

We don't believe that one size fits all. Nor are we influenced by what others do. From policy inception through to claims settlement, we apply our energy and expertise to really understanding our clients' needs. It's this attention to detail that enables us to tailor the solution that's exactly right for them.

QBE for SME

We want to make it as easy as possible for you to win more business by giving you:

- Flexible, tailored products specially designed for SMEs
- Direct access to empowered underwriters
- An 'open for business' attitude to risk and rates

Standard cover

Data security and multimedia cover

- Including voice/telephony/telephone hacking (sub limit £25,000)
- Liability arising out of multimedia exposures as a result of a hacker. For example defamation, libel and infringement of intellectual property rights
- Liability arising from the failure to properly handle, manage, store, destroy or otherwise control personally identifiable information
- Liability arising out of unintentional transmission of a computer virus
- Liability arising out of a hacker's fraudulent use of information
- Loss of money, property or products that has been transferred to a third party via unauthorised access, including damage to stock stored in temperature controlled environments (sub limit £100,000)
- The costs to withdraw or alter data or images or other website content as a result of a court order or to mitigate a claim (up to the policy limit or maximum £500,000, whichever is lower)
- The costs to replace or restore documents discovered by the insured to be lost, damaged or destroyed (sub limit £100,000)
- Compensation costs arising as a result of directors, partners and employees attending court in connection with a covered claim
- Defence costs.

Policy limits of indemnity of £100,000, £250,000, £500,000, £1 million, £2 million and £5 million available.

Social Engineering Fraud cover

- Covers theft of money, property, funds or tangible securities using fraudulent methods
- Social Engineering Fraud cover included as standard where risk information is acceptable, with the sub-limit of indemnity being 10% of the cyber policy limit of indemnity or £100,000 whichever is lower
- The social engineering fraud limit can be increased if Crime cover is taken but limited to 50% of the Crime limit of indemnity or £250,000 whichever is the lowest.

Data breach notification costs cover

- The provision of consumer notifications to comply with data breach law following a data breach
- The legal fees incurred to identify notification communication obligations and draft notification communications
- The costs to send and administer notification communications
- The costs of call centre services to respond to enquiries and queries following a notification communication.

Information and communication asset rectification costs cover

- The costs for repair, restoration or replacement of computer and telecommunication system software and hardware, damaged, destroyed, altered, corrupted, copied, stolen or misused by a hacker.

Regulatory defence costs cover

- Payment for those amounts which the insured is legally obliged to pay (including legal and defence costs) as a result of a civil regulatory action, regulatory compensatory award, civil penalty, or fines to the extent insurable by law, imposed by a government or public authority regulator
- Cover for Payment Card Industry (PCI) fines and legal investigation costs (limit £50,000).

Public relations costs cover

- Payment for all reasonable costs the insured incurs for a public relations and crisis management consultant to avert or mitigate any material damage to any of the insured's brands and business operations (sub limited to £100,000).

Forensics costs cover

- Payment for a forensic consultant to establish the identity or methods of the hacker or other details required by the insurer following a data breach
- Payment for a security specialist to assess the insured's electronic security and the costs of reasonable security improvement
- Payment for the temporary storage of the insured's electronic data at a third-party host location, if it is viewed that the insured's information and communication assets remain vulnerable to damage, destruction, alteration, corruption, copying, stealing or misuse by a hacker.

Credit monitoring costs cover

- Payment for credit monitoring services in order to comply with data breach law.

Cyber extortion cover

- Payment for reasonable and necessary expenses incurred by the insured including the value of any ransom paid by the insured for the purpose of terminating a cyber-extortion threat.

Optional cover

Cyber Business Interruption cover

- Payment for loss of business income (net profit), as a result of the total or partial interruption, degradation in service, or failure of information and communication assets following a failure by the insured or a service provider to protect against unauthorised

access to, unauthorised use of, a denial of service attack against, or transmission of a computer virus to, information and communication assets

- Maximum indemnity period 3 months
- Time excess (waiting period) 6-18 hours dependant on the trade selection.

Full Crime cover

- Theft or criminal damage of money, tangible securities, property or funds of the insured or their clients, by any third party or any employee or any employee acting in collusion with a third party.
- Crime policy limits of indemnity of £100,000, £150,000, £250,000, £350,000 and £500,000 available.

We're particularly good at covering:

- Contractors
- Manufacturing and wholesaling industries
- IT, including consultancy, programming, data processing and gaming
- Advertising and marketing
- Agricultural and farming
- Business consultants
- Catering
- Residential property management, estate agents and letting agents
- Planning, design and surveyors
- Engineering
- Marine
- Mechanics
- Warehousing, storage and cold storage
- Motor and caravan industry
- Amateur sports clubs
- Libraries
- A range of bespoke/niche professions

Some areas where this product isn't suitable are:

- Education
- Healthcare and social services
- Financial institutions
- Telecommunications
- Energy, oil, gas and utilities



Get a quote or more information

QBE FastFlow

Web: fastflow.qbe.com
Email: SMEcommercial@uk.qbe.com
Phone: 0800 917 9369

Acturis

Category: **Liability**
Policy Type: **Liability Combined**
Product Target: **Cyber Package**
Email: SMEnew@uk.qbe.com
Phone: 0800 917 9362

Intended for broker use only. Please refer to our policy wordings for full terms and conditions and any exclusions that may apply.

Disclaimer

This publication has been produced by QBE Insurance (Europe) Ltd (QIEL). QIEL is a company member of the QBE Insurance Group. Readership of this publication does not create an insurer-client, or other business or legal relationship.

This publication provides information about the law to help you to understand and manage risk within your organisation. For full details of the disclaimer surrounding this publication please visit QBEurope.com/legal/publication-disclaimer.asp

QBE Insurance Group Plantation Place 30 Fenchurch Street London EC3M 3BD
tel +44 (0)20 7105 4000 QBEurope.com

8958/CyberCrimeProductSheet/JUN2018 QBE European Operations is a trading name of QBE Insurance (Europe) Limited and QBE Underwriting Limited, both of which are authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.

Made possible
