CyberCrime

Cyber criminals are increasingly targeting small and medium-sized businesses. Our CyberCrime product is tailor-made to provide the comprehensive cover SMEs need to keep them safe.

Reflecting our pioneering role in developing innovative e-trade products that go that one step further, our CyberCrime product was the first of its kind offered through the Acturis platform.

This product is suitable for almost every kind of business and includes cover for Social Engineering Fraud as standard. We can also include Cyber Business Interruption cover and full Crime cover for added peace of mind.

Main benefits

> Fast e-trade quotes for around 3600 trades and professions, 24 hours a day.
> Social Engineering Fraud cover Optional Extra where risk management acceptable (theft of money, property or goods by using fraudulent methods such as fake emails and phone calls).

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.

> Core cyber covers included as standard
- Cyber Liability including data security and multimedia.
- Data breach notification costs
- Information and communication asset rectification costs
- Regulatory defence costs, including cover for Payment Card Industry (PCI) fines and legal investigation costs
- Public relations costs
- Forensics costs
- Credit monitoring costs
- Cyber extortion

> 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

QBE cyber risk management portal

Customers have free access to the QBE Cyber Risk Management Portal, which offers a wide range of information on cyber risks and how to make sure you're protected against them. See eriskhub.com/qbe.

Standard cover

Data security and multimedia cover

- 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
- Policy limits of indemnity of £100,000, £250,000, £500,000, £1 million, £2 million and £3 million available.

Social Engineering Fraud cover

- Covers theft of money, property, funds or intangible 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 £50,000 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 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.

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 to protect against unauthorised access
> 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

> Social engineering fraud
> Cyber business interruption
> Crime
> Data security
> Cyber extortion.

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

QBE FastFlow

fastflow.qbe.com
SMEcommercial@uk.qbe.com
0800 917 9369

Acturis

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

QBE European Operations

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

375760_6_2203