

Protect your business

Cyber criminals are increasingly targeting small and medium-sized businesses as a stepping stone in order to gain access to the large organisations that they work with or supply.

A tailored insurance policy can cover your business for many of the main cyber and crime risks, including:

Social Engineering Fraud, where money, property or goods are stolen through methods such as fake emails and phone calls



Cyber extortion, where criminals threaten to make sensitive information available on the Internet or to competitors

Public relations help to protect your company and brand reputation

Forensics, data breach notification and credit monitoring costs

Ransomware that locks your computers and brings business to a standstill



Compensation costs if directors, partners and employees need to attend court in connection with a covered claim

Telephone hacking

Fraudulent websites

Loss or damage to documents

Computer viruses and malware



Damage to stock or goods stored in temperature controlled environments as a result of a cyber incident

Restoration or replacement of website / digital media maintained by a third party

Damage or theft of computer equipment

Business interruption and downtime

We encourage all businesses to analyse all the risks:

- Securing IT networks and systems
- Protecting customer data
- Safeguarding intellectual property and trade secrets
- Securing your business premises with alarms and CCTV
- Minimising business interruption and downtime
- Reducing the risk of any financial penalties
- Reducing reputational damage and a public relations crisis

And to have robust IT processes

- Use a firewall on your computer network
- Encrypt all sensitive data
- Keep software updated
- Use up-to-date antivirus software and subscribe to a threat alert service
- Avoid using easy passwords
- Discourage staff from bringing in their own devices
- Backup your data regularly



Delete suspicious emails without opening

Be wary of clicking on links in emails

Test your website and web hosting for any vulnerabilities

Invest in a shredder and securely dispose of documents

Securely dispose of old laptops and computers by wiping their hard-drives

Secure portable devices such as laptops, mobile phones and USB memory sticks

Consider a basic cyber incident response plan

Tip! Businesses like to deal with people that won't let them down, so showing that you're taking the cyber threat seriously can help you be seen as being reliable to deal with.

Get extra peace of mind with QBE CyberCrime Insurance

As business insurance specialists, QBE's new CyberCrime insurance policy has been specially designed to provide SMEs with comprehensive insurance cover and a rapid forensic response to help get you back up and running quickly in the event of an incident.

Ask your broker for a quote for QBE CyberCrime insurance.

QBE for SME
www.QBEurope.com/sme

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