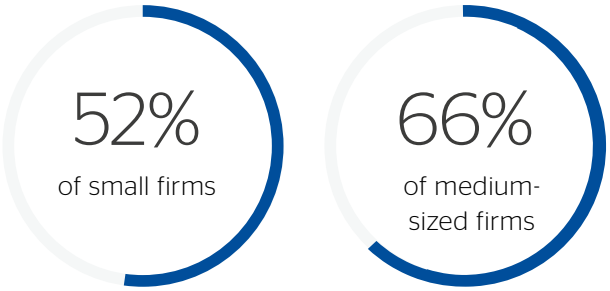
QBE CyberCrime

What's the risk to your business?

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

Virtually all UK businesses use computers and online services and are exposed to cyber risks through:

- email
- websites
- social media
- online banking



have been the victim
of at least one cyber breach in the last 12 months.

Common types of cyber attacks

- Fraudulent email
- Viruses and malware
- Phoney websites
- Ransomware
- Impersonation fraud

A cyber incident can lead to:

- Theft of money, data or goods
- Business interruption
- Reputational damage to your company or brand

The scale of the threat is increasing.
It's no longer safe to think "It will never happen to us..."

Cyber crime costs UK businesses £20 billion per year

What would the cost and the impact be if your business was down for a few days, a week or longer?

Made possible
QBE

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

Protect your business...

Cyber crime is one of the biggest risks facing businesses of all sizes today.

- 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.QBEeurope.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 QBEeurope.com/legal/publication-disclaimer.asp

Made possible QBE

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

QBE European Operations is a trading name of QBE UK Limited, QBE Underwriting Limited and QBE Europe SA/NV. QBE UK Limited and QBE Underwriting Limited are both authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and Prudential Regulation Authority. QBE Europe SA/NV, VAT BE 0690.537.456, RPM/RPR Brussels, IBAN No. BE53949007944353 and SWIFT/BIC No. HSBCBEBB, is authorised by the National Bank of Belgium under licence number 3093.

156272/MAR19