QBE CyberCrime

We've got you covered - some claims examples

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.

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

Computer lockdown

A company director at a construction firm quite innocently clicks on a link in an email that he believes has come from one of his customers. To his horror his computer and the company's entire computer network are instantly locked with a message demanding a ransom payment of £2000 in bitcoin to restore things back to normal.

Denial of service

A small online retailer makes the majority of their turnover in small windows of time, with seasonal goods. When their e-commerce website crashes it is suspected that a competitor has used a 'botnet' to shut the business down during a busy period, leading to severe business interruption and substantial impact on company finances.

In the cloud

A manufacturing company stores all their data offsite via a cloud provider. This includes sensitive customer, employee and financial data. Over the weekend they learn that someone, who they believe may be a disgruntled ex-employee, has been able to access the account and now has control of their entire data and is effectively holding them to ransom to get it back.

Friday fraud

Just before the weekend an employee in the accounts department receives what appears to be a genuine email from one of their longstanding customers, to ask if a payment can be made that same day to 'help them out of a cashflow problem'. The email gives a bank account number and sort code for the payment. Needless to say, the money has just gone to a scammer.

Missing money

The book-keeper in a small IT firm is surprised to see several unaccounted-for payments going out of the company bank account. Unwittingly, she had clicked a link in an email a couple of weeks ago which had downloaded a piece of 'keylogging' malware onto her PC. Criminals have been able to record every key she pressed on her computer keyboard and have access to her passwords, customer data and the bank account logon details.

Notifying customers

Following a cyber attack a retailer has to notify all customers affected that their personal information, including credit card details, may have been hacked. As well as the cost of sending out thousands of notifications, over the next few days the company is inundated with telephone calls and emails and has to cope with increased workloads to handle the volume of enquiries.

Employee crime

The owner of a small wholesaler has noticed small amounts of money going missing over several months. Investigations lead to an employee who has had his 'fingers in the till' for almost a year.

Frozen food

A cold storage facility endures two days of business downtime and is forced to write off thousands of pounds worth of stock that has defrosted due to their warehouse management computer system being hacked.

Not good for PR

Customers take to social media and the press to complain about their personal data being hacked. The company is lambasted on Twitter and Facebook for their 'shoddy handling' of the whole affair and resorts to hiring in a professional public relations crisis management company to restore confidence.

A cyber incident can lead to:

Theft of money, data or goods

Business interruption

Reputational damage to your company or brand

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

It's no longer safe to think "it will never happen to us..."

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

Made possible QBE

8126CC/CyberCrimeClaimsExamples/AUG2017