Cyber claims scenario
Phishing - Cybercrime

In the dynamic threat landscape of cybercrime, criminals are now employing a variety of sophisticated techniques, such as malware, ransomware, and social engineering (e.g. phishing), making businesses of any size or industry susceptible to attacks. Most cyber incidents stem from human error, and as cybercriminals refine their methods, detecting a fraudulent third party attempting to access your system is becoming increasingly harder to spot.

Phishing

Incident

Fraser, a small business owner, receives an email from one of his suppliers requesting a BACS payment of £5,000. He emails the supplier to verify bank details and receives a reply confirming all is in order to proceed. He makes the payment. Four days later, Fraser receives another email from the same supplier querying where the now overdue payment is.

Response

Fraser notifies his insurer and their investigators work with the company's IT team. They identify a suspicious spam email which has led to Fraser's email account being compromised. The investigators discover the rules for the account have been set up to forward emails to an unknown external account, which means the original supplier email has been intercepted and incorrect bank details provided to Fraser.

Outcome

Fraser notifies the relevant authorities and the business's bank, but unfortunately the money cannot be traced. Due to Fraser having a cybercrime extension on his existing Cyber insurance policy, his total claim cost of £6,000 (including £1,000 of forensics fees) was covered.

Risk less

In association with AVIVA

Key takeaways

The fourth emergency service

Cyber Insurance policies are the fourth emergency service, designed to provide high-levels of emergency support when you need it most. Phishing is one of the most common and claimed-for types of cybercrime and many people don't realise that if they were victims of a phishing scam, a standard cyber policy wouldn't pay out.

Cybercrime extension

A Cybercrime extension can be added to a standard cyber insurance policy, offering additional protection against fraudulent electronic invoicing, fraudulent electronic funds transfers, and fraudulent emails (phishing).

How to be more 'Cyber aware'

Speak to your broker

Whether you're a newbie to Cyber Insurance, or you'd like to increase your level of cover, your broker has the expertise to provide you with the most cost-effective option that caters to your specific cyber needs.

Humans are the weakest link

Human error accounts for the majority of cyber-attacks, so it makes sense to do everything you can to lessen the risk (or you could end up being the weakest link in your cyber security). Test your employees with mock phishing emails and and look out for news-jacking where hackers send timely and topical scams that feel relevant.

EMAIL
info@macbeths.co.uk

VISIT
macbeths.co.uk

CALL
0118 916 5480

Macbeth Insurance Brokers and Aviva are working together to help protect businesses against the risk of underinsurance.

The scenario shown in this document is fictitious and has been used for illustrative purposes only.