10 REASONS FOR CYBER INSURANCE

"My company is too small to be a target for a cyber attack"

"I already have a computer policy so I don't need cyber insurance"

"I already have anti-virus software"

These are common misconceptions when considering cyber insurance.

Here are 10 reasons your clients may benefit from cyber insurance.

CLAIMS EXAMPLE

Sensitive data left on bus

An employee for a company left a laptop on a bus. The files on the computer contained sensitive customer data. Action had to be taken quickly to ascertain what happened. The client was guided through the security breach process, action protocols were created, and specialist IT companies were mobilised along with PR consultants. The client's customers felt the matter was dealt with well, and no further issues arose. As a result, no third party claims were made.

CLAIMS EXAMPLE

Distributed denial of service task

A ransom email was sent to a company advising that a denial of service attack (DDoS) was imminent. There was a demand for payment to be made otherwise the DDoS attack would be set in motion and the client would be locked from using their systems. A cyber response coach cooperated with IT professionals and Government authorities to prevent the attack. Also, IT specialists isolated any impact ensuring no loss was caused, and Government authorities were able to trace the attacker and prevent other attacks from occurring.

HERE ARE 10 REASONS YOUR CLIENTS MAY NEED CYBER INSURANCE.

01 BUSINESS MAY GRIND TO A HALT

With most organisations heavily reliant on technology to conduct everyday business, inaccessibility of IT systems due to a cyber attack or data breach can result in severe business interruption to both first and third parties. A comprehensive cyber insurance policy will include cover for loss of profits, internal errors and unexpected technical failures.

02 A CYBER ATTACK CAN BE COSTLY

In addition to 'surface' costs (customer breach notifications, regulatory compliance fines and technical investigation costs), organisations may also incur less visible costs, such as lost contract revenue or loss of intellectual property, for which a cyber policy may offer cover. The average cost of UK cyber crime increased by 31% between 2017 and 2018[1], costing the UK economy around £11bn.

03 PEOPLE MAKE MISTAKES

More than a fifth of data breaches occur as a result of human error or negligence[2], such as loss of a device or a stolen laptop containing sensitive data. Other examples include employees using personal USB sticks or clicking links within SPAM emails.

04 REGULATORS CAN LEVY HEFTY FINES

With increasing focus on data protection regulation, such as GDPR, cyber insurance may include cover against defence costs, fines and penalties following unauthorised disclosure of personal and/or confidential information.

05 A COMPANY'S REPUTATION MAY BE DAMAGED

Where a company's reputation is threatened following an attack or breach, a comprehensive cyber policy will cover the cost of a consultant to help minimise damage to reputation and brand.

06 COMPUTER INSURANCE ALONE WON'T COVER LOST DATA

Computer insurance may cover damage to hardware but not software. A reputable cyber insurance policy will cover costs required to restore data system functionality and lost data, helping to get systems and networks back up and running swiftly.

07 ANY BUSINESS CAN BE A TARGET

Cyber criminals don't discriminate by company size or type. In 2018, 31% of micro and small businesses and 61% of large firms identified breaches or attacks.[3] Therefore any business which stores digital data can be at risk of an attack or data breach.

08 ACTING FAST IS KEY

Cyber insurance may include cover to pay for forensic experts to identify, contain and remove the threat. The sooner this is done the better. Ponemon Institute research[4] reported that companies which contained a breach in fewer than 30 days saved over $1 million as compared to those that took more than 30 days to resolve the incident.

09 CYBER INSURANCE REASSURES THIRD PARTIES

Taking out cyber insurance can send a clear message to customers and suppliers that a company takes IT security seriously and has protection in place to manage an incident in the event of a breach. This assurance can be a selling point for companies looking to qualify for bids and tenders.

10 CYBER CRIME IS INCREASING

The most common fraud in the UK in 2018 was cyber crime[5] and cyber incidents topped the Allianz Risk Barometer 2019 as a key corporate peril for UK businesses. Generally, cyber attacks are on the increase[6] so it's more important than ever for companies to take measures to protect themselves. Cyber insurance can offer such protection, in combination with robust risk management strategies.

1 Accenture & Ponemon Institute (2019). The Cost of Cyber Crime: Ninth Annual Cost of Cybercrime Study. [online Available at: https://www.accenture.com/us-en/insights/security/cost-cybercrime-study [Accessed 16 Aug. 2019].
2 Ponemon Institute. 2018 Cost of a Data Breach Study: Global Overview. July 2018
3 Cyber Security Breaches Survey 2019. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2019
4 2018 Cost of a Data Breach Study: Global Overview. Ponemon Institute
5 PwC's Global Economic Crime Survey 2018: UK Findings. 2018
6 ibid.

ACOM8435_5 08.20

Allianz