Global Cyber and Technology

The 10 Most Common Cyber Insurance Questions

01 What is cyber risk and cyber risk management?

Cyber risk can be defined as any kind of risk that emerges from the use of information and communication technology. Cyber risk management focuses on risk control and prevention and includes risk avoidance, risk mitigation and risk transfer (i.e. cyber insurance).

02 What is cyber insurance?

Cyber insurance protects businesses from risk relating to IT infrastructure and activities. It covers risks resulting from some malicious attacks as well as some inadvertent incidents which can cause harm to a business's computer network or to its business data. Cyber insurance will generally reimburse some of the business's own costs of dealing with the cyber event, but will also cover liability to third parties that emanates from the event. A significant benefit of a cyber policy is the breach response services provided, whereby the insured gets immediate access to expert consultants; very welcome help when the business is in a particularly vulnerable position. Cyber threats create considerable pressure, confusion and concern and having immediate access to a breach response team which includes IT forensics, lawyers as well as PR and crisis management consultants, can assist the business in good decision-making. Access to experienced ransom negotiators is also often provided.

Cyber policies extend to reimbursing the insured for expenses in dealing with the breach, dealing with the resultant damages and defence costs of third party liability.

03 My IT security is great. Why do I need cyber insurance?

No matter how much a company invests in IT security, a business will never be 100% secure. Furthermore, no fire wall or virus protection will protect against human error or a rogue employee.

If your business handles sensitive customer data or if your business is reliant upon computer systems to operate, then some consideration of cyber insurance is critical. IT security is one part of the puzzle; cyber insurance is another. They are not mutually exclusive and should go hand-in-hand at all times.

04 We outsource our IT so where is our cyber exposure?

Even if you outsource your IT, the chances are your business will remain liable. Your firm will still have obligations to keep client data safe, and to ensure that the business is able to operate. Your business's fiduciary duties to clients do not disappear, nor does the need to access data or maintain network systems for continuity of operations. While it might be possible to claim damages successfully from your IT supplier for a breach by that supplier, relying on that outcome alone would be unwise.

05 We don't collect any sensitive data. Why do I need cyber insurance?

Any business that relies on a computer system to operate is at risk. Cyber risks don't just involve data breaches. Other risks to businesses include system security breaches (such as ransomware, transmission of malicious code, denial of service attacks).

06 Our business is relatively small. Don't hackers just target big companies?

Ransomware attacks are increasing exponentially. While hackers target vulnerable businesses of all size, recent trends show that 43% of cyber - attacks are targeted towards SMEs. Further, cyber incidents are not all criminally motivated. Inadvertent data breaches or mistakes can happen to businesses of any size.

07 My business is not in a risky industry sector so why do I need cyber insurance?

Simply put, all industries are at risk. Every business has assets of value which can be leveraged by cyber criminals. Equally, computer viruses are indiscriminate in their ability to move across networks, irrespective of the nature of the business transacted over that network.

LOCKTON®

UNCOMMONLY INDEPENDENT

Lockton Companies LLP
Authorised and regulated by the Financial Conduct Authority. A Lloyd's broker.
Registered in England & Wales at The St Botolph Building, 138 Houndsditch, London EC3A 7AG.
Company No. OC353198.

08 My cyber risk is already covered by other more traditional lines of insurance, isn't it?

Many people mistakenly believe that cyber cover may already be addressed in other insurance policies they have purchased. Some overlaps exist (as they do with all lines of insurance) but traditional insurance policies lack the depth and breadth of standalone cyber cover, and won't come with experienced cyber claims and incident response capabilities.

09 Will my cyber policy actually work and respond when I need it to?

There is a myth in the market place that cyber policies don't respond. We believe this myth has arisen as a legacy of the earliest cyber policies developed some 20 years ago. An insured business was often required to ensure strict security, network and data maintenance controls remained in place or else risk the policy's coverage. A lot has changed since then and most policies no longer include such obligations.

A recent report highlights that 99% of claims made on its member insurance policies* in 2018, were paid. Cyber insurance policies have one of the highest claims acceptance rates across all insurance products.

10 How do cyber policies cover employees working from home?

Many concerns have recently been around remote working environments. Employees working from home create a potential issue regarding whether their personal computer is part of a company's computer system for purposes of cyber coverage. 'Computer System,' or words to that effect, are typically defined in a policy. Many policies encompass remote working arrangements to fall under this definition. The definition of 'Insured' also commonly includes employees working on behalf of the insured. The issue should be clarified with your broker prior to inception of the policy.

Vanessa Cathie
Account Executive
T: +44 (0)20 7933 2478
M: + 44 (0)7780 487830
E: vanessa.cathie@uk.lockton.com

*: https://www.abi.org.uk/news/news-articles/2019/08/cyber-insurance-payout-rates-at-99-but-uptake-still-far-too-low/