COMPOSITION OF A CYBER POLICY

We've broken down a cyber policy to show you how it works

Cyber insurance policies tend to be modular in nature, meaning that they consist of a variety of different coverage areas and, for many, that has led to confusion around how exactly this cover fits together to create a uniform whole. To help explain this further, we've broken down the basics of a cyber policy into their core sections to show how each part of the coverage functions.

Cybercrime

In the context of a cyber insurance policy, cybercrime usually refers to attacks that involve theft of funds from the victim as opposed to theft of data or other digital assets. This usually happens in one of three ways:

• **Extortion**, where hackers use the threat to expose or destroy data that they have already compromised in order to extort money out of the victim;

• **Electronic compromise**, where attackers manage to hack into the insured's network and gain access to their online accounting or banking platforms; or

• **Social engineering**, where attackers imitate a senior executive or third party
Media liability

Contact us – engage@neuro8.com

A media liability section covers any third party claims arising out of defamation or infringement of intellectual property rights. Media cover started out in cyber policies to offer protection in respect of online content only, but as policies have broadened over the years, it's not uncommon for full media cover to be provided.

Incident response

Incident response is at the heart of any good cyber policy. This section of cover will generally pick up all of the costs involved in responding to a cyber incident in real time, including IT security and forensic specialist support, gaining legal advice in relation to breaches of data security, and the costs associated with having to notify any individuals that have had their data stolen. One of the most important aspects of a cyber policy is that it provides speedy access to the right specialists as well as paying for their services.

System damage and business interruption

What really gives a cyber policy its grounding is a strong system damage and business interruption section. Helping to keep your business up and running, this crucial section covers the costs for an insured's data and applications to be repaired, restored or recreated in the event that their computer systems are damaged as a result of a cyber event. It also reimburses the loss of profits and increased cost of working as a result of interruption to a business' operations caused by a cyber event or prolonged system downtime.

Network security and privacy liability

Network security and privacy liability is an important part of a cyber policy. This section covers third party claims arising out of a cyber event, be it transmission of harmful malware to a third party's systems or failing to prevent an individual's data from being breached.

Make sure your policy fits your needs

It is very common for any one claim to trigger multiple sections of cover, so ensure your policy adequately addresses the most critical areas of coverage – namely the first party sections like incident response, cybercrime and system damage and business interruption – and that these are available on an unlimited reinstatement basis. First party losses accounted for a staggering 95% of insurers cyber claims last year, and the nuances of coverage within these sections can mean the difference between a weak policy that doesn't perform when put to the test, and a fit and healthy policy that can endure multiple blows but stays on its feet.

Contact us – engage@neuro8.com