# What makes up a cyber policy

Cyber insurance policies tend to be modular in nature, meaning that they consist of a variety of different coverage areas.

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 dissected our cyber policy section by section to show how each part of this body of coverage functions.

## Key – types of coverage

Most cyber policies can be divided into two areas – first party covers and third party covers.

1st **The first party sections** cover the insured's own financial loss arising from a cyber event, which is defined as any actual or suspected unauthorised system access, electronic attack or privacy breach, or system downtime. It's important to note that the vast majority of cyber claims stem from first party losses.

3rd **The third party sections** cover the insured for liability actions against them arising out of a cyber event.

## 1st 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.

Look for ▶ insurance providers that have a proven track record of responding to claims, an in-house cyber claims team as this can speed the process up considerably, and specialists local to the policyholders they cover within their partner network.

## 1st System damage & business interruption

Helping to keep your business up and running, th crucial system damage and business interruption 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.

Look for ▶ cover that is not only triggered by malicious cyber events but also by accidental system failure, meaning that a cyber event does not have to take place in order for cover to apply. Also see if the section addresses consequential reputational harm.

## 1st Cybercrime

Within 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
- Social engineering, where attackers imitate a senior executive or third party

Look for ▶ policies that cover the full range of cybercrime types, from funds transfer fraud and ransomware to targeted extortion and the unauthorized use of computer resources through cryptojacking or botnetting. Ask your underwriter if any risk management warranties apply.

## 3rd Media liability

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, it's not uncommon for full media cover to be provided.

## 3rd Network security & privacy liability

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.