

# Five overlooked features of cyber insurance

With a multitude of cyber insurance products available in the UK a lot of work has been carried out on policy comparisons, but there are some product characteristics that are often overlooked or require further examination. Here are five key features and why they're important:

## 1 Implementation of Immediate Incident Response.

Speed and professionalism are key and having the right experts involved at the beginning of a cyber event is crucial. How quickly is the insured speaking to that expert and what are the steps for the all-important first few hours? With sensitive information, it's also a bonus to be speaking under legal privilege. Having a £0 deductible for this immediate response also enables quick handling (without the insured hesitating over whether they will have to pay an excess amount for initial fees).

## 2 'Discovery' Language.

What happens if a cyber event/issue is lying undiscovered in the insured's system prior to first purchasing cyber cover? How does the cyber policy respond to this discovery? Be wary of policies that potentially refuse cover (or use language such as 'ought to have known'). A policy that provides cover for when a cyber event is first discovered is a positive feature.

## 3 'Cyber Crime' Cover.

This is becoming more commonplace, but be wary of policies that use cyber-only triggers. Fund transfer fraud or social engineering fraud can still be carried out by methods that don't involve the insured's systems or unauthorised access. A limited policy trigger can leave gaps in cover.

## 4 'Potential/suspected' Language.

With a cyber event, quite often it's not known if information has fallen into the wrong hands or there has been an actual unauthorised access. Rather than putting the onus on the insured to prove this, look for a policy that uses 'potential' or 'suspected' language in relation to the coverage trigger.

## 5 'Pay on Behalf of' Language.

Many cyber insurance policies provide good 1st party coverage or incident response costs, but on a reimbursement basis, meaning the insured must incur the costs and then claim the money back. 'Pay on behalf of' language ensures a smooth process that doesn't financially inconvenience the insured.

*Most cyber policies should reimburse an organisation for costs and liabilities incurred in dealing with the fallout of a cyber event. But a good insurance product should do much more than that. It is not just about checking what's covered by a policy, it's about understanding how implementation occurs.*

To be solid, insurance must be flexible